

EXHIBIT 3



AUTORITEIT
PERSOONSGEGEVENS

Personal Data Authority

P.O. Box 93374, 2509 AJ The Hague
Hoge Nieuwstraat 8, 2514 EL The
Hague T 070 8888 500 - F 088
0712140
autoriteitpersoonsgegevens.nl

Confidential/Signed

[confidential]

Date

July 22, 2024

Our reference

[confidential]

Contact

[confidential]

Subject

Decision imposing administrative fine

Dear [confidential],

The Personal Data Authority (AP) has decided to impose an administrative fine of **€290,000,000** on Uber Technologies Inc. and Uber B.V. (hereinafter collectively referred to as Uber). The AP believes that Uber violated Article 44 of the General Data Protection Regulation (GDPR) because Uber allowed transfers of personal data to the United States while not providing appropriate safeguards as stipulated in Chapter V of the GDPR.

The AP believes that imposing an administrative fine on Uber is not only appropriate but also necessary. This is because the AP has found that the intended interest of Article 44 GDPR, namely the continuity of the high level of protection of the GDPR when transferring personal data to third countries, is not guaranteed by Uber. The AP considers this serious and for this reason has taken enforcement action against Uber.

This decision explains the administrative fine. To this end, it deals successively with the reason for the investigation, the facts, the violation found and the amount of the fine. Finally, the dictum follows.



Date

July 22,

Our

reference

Contents

Contents	2
1. Reason for research	4
2. Facts and circumstances	5
2.1 Introduction	5
2.2 Uber drivers and the driver app	5
2.3 The processing activities	7
2.4 Number of Uber drivers and GDPR requests from data subjects	12
2.5 Uber's application of a transfer tool	12
3. Views of Uber	13
4. Review	16
4.1 Processing of personal data	16
4.2 Controller and authority AP	16
4.3 Territorial scope and Chapter V GDPR	17
4.4 Is there any transfer of personal data?	20
4.4.1 Legal framework	21
4.4.2 Review	22
4.4.3 Conclusion	28
4.5 Did Uber have a transfer tool?	29
4.5.1 Legal framework	29
4.5.2 Review	30
4.5.3 Conclusion	31
4.6 Can Uber successfully invoke a Section 49 GDPR exception?	32
4.6.1 Legal framework	32
4.6.2 Review	33
4.6.3 Conclusion	39
4.7 Final conclusion	39
5. The fine	39
5.1 Penalty power and view of Uber	39
5.2 Systematic determination of penalty level	41



AUTORITEIT
PERSOONSGEGEVENS

Date	Our	
July 22,	reference	
5.3	Penalty amount calculation	41
5.3.1	Step 1: Identify acts and violations	41
5.3.2	Step 2: Determine starting amount	42
5.3.3	Step 3: Assess other relevant circumstances	46
5.3.4	Step 4: Checking exceedance of maximum amounts applicable to violations.....	46
5.3.5	Step 5: Assessing requirements of effectiveness, proportionality and deterrence	46
6.	Decision.....	48



Date
July 22,

Our
reference

1. Reason for research

1. Uber is an international company that acts, among other things, as an intermediary between cab drivers and passengers. Passengers use the general Uber App (for cell phones) or possibly a browser to book a ride. Drivers use the Uber Driver App (hereinafter: driver app) to offer rides.
2. Use of the driver app requires drivers to create an account. Drivers are rated by their customers after a ride and paid by Uber for services rendered.
3. On June 12, 2020, the Commission Nationale de l'Informatique et des Libertés (CNIL) received a complaint from the French non-governmental organization Ligue Des Droits De L'homme Et Du Citoyen (LDH, hereafter: complainant) on behalf of 21 Uber drivers. Gradually, another 151 Uber drivers joined the complaint, making it on behalf of 172 complainants. LDH then filed an additional complaint with the CNIL on September 29, 2020, which was forwarded to the AP on January 11, 2021.
4. In this supplemental complaint, the complainant argues that Uber's legal position is not clear as a result of the so-called SCHREMS II ruling of the Court of Justice of the European Union (hereinafter: ECJ). In the SCHREMS II ruling, the ECJ stated that there is no equivalent level of protection in the United States for the transfer of personal data from the European Union ("EU") to the United States. As a result, the adequacy decision with the United States ("*Privacy Shield*") was no longer valid as an instrument for the transfer of personal data. The CJEU did indicate that "*Standard Contractual Clauses*" (SCC) did allow the continued transfer of data to the United States, provided sufficient additional measures were taken to ensure an equivalent level of protection.¹
5. On April 16, 2021, the AP notified Uber in writing that it had launched an investigation following complaints filed by French Uber drivers. This investigation focused on whether Uber complied with the stated requirements of Chapter V GDPR for the transfer of personal data of drivers from the EU to the United States.
6. The AP's investigation subsequently found a violation of Article 44 of the GDPR, as Uber allowed transfers of personal data to take place while not providing appropriate safeguards as stipulated in Chapter V of the GDPR. The investigation report was sent to Uber by letter dated April 13, 2023. Uber submitted a view on the investigation report by letter dated June 9, 2023. On July 5, 2023, Uber orally explained its views during a views session at the AP's office.

¹ CJEU July 16, 2020 - Data Protection Commissioner v. Facebook Ireland Ltd. and Maximilian Schrems, C-311/18.



Date

July 22,

Our

reference

2. Facts and circumstances

2.1 Introduction

7. Uber is the name of an electronic platform developed by Uber Technologies Incorporated (hereafter UTI). UTI's principal place of business is San Francisco, United States. The Uber platform is represented in the European Economic Area (hereinafter: EEA) by Uber B.V. (hereinafter UBV). In the cities where Uber operates, Uber enables passengers to order transportation services through the Uber platform. One can request a ride with Uber in various European cities and countries, and Uber has drivers operating in those territories.²
8. According to Uber's privacy statement, UBV and UTI are joint controllers for the processing of personal data of Uber drivers in the EEA territory.³ Their responsibilities regarding compliance with obligations under the GDPR are outlined in an agreement.⁴
9. UBV has several data processing agreements with other Uber subsidiaries in EEA countries. For example, with respect to Uber France SAS, Uber's subsidiary in France, it identifies UBV as the data controller and Uber France SAS as the processor.⁵ The data processing agreement states that within this interrelationship, UBV is the entity that makes Uber drivers' personal data available to other Uber subsidiaries in the EEA. However, in a clarification, Uber indicated that while UBV is responsible for Uber drivers' personal data in the EEA, technically it is accessed by UTI.⁶
10. Uber drivers in the EEA must sign a contract with UBV to become a driver with Uber.⁷

2.2 Uber drivers and the driver app

11. Uber describes drivers as "*users of the platform who provide transportation services individually or through partner transportation companies using the Uber Driver application.*"⁸ To become an Uber driver, one must

² File 20, Locations of Uber.

³ The Uber privacy statement is available at: <https://www.uber.com/legal/en/document/?name=privacy-notice&country=netherlands&lang=nl>

⁴ Uber Data Sharing Agreement between Uber B.V. and Uber Technologies Inc. Scope: Uber Personal Data c Employee Data closed on August 6, 2021.

⁵ File 17, Response to Intelligence Request 2, Attachment Processing Agreement Uber France SAS.

⁶ See the minutes of the view session held on July 5, 2023.

⁷ File #4, Uber Additional Terms for Drivers.

⁸ In response to the information request dated July 7, 2021, Uber B.V. provided their records regarding Driver Personal Data Processing Activities to the AP on August 9, 2021. What is meant by this is stated under 'III. Categories of Data Subjects Whose Personal Data Uber Processes'.



Date

July 22,

Our

reference

create an account on the driver app.⁹ In addition, to gain access to the platform, the driver must accept the "*Conditions for independent Uber Partners*."¹⁰ These conditions can be changed unilaterally by Uber.¹¹ After fulfilling the conditions and logging into the app, the driver can "go online. Then the driver can accept, decline or ignore rides (requested by passengers located near him). A driver who is online, but who decides to ignore a requested ride three times in a row, is automatically logged off the platform. However, the driver still retains access to the other facilities on the platform. It should be noted that a driver has the option to cancel a ride he has already accepted. Regarding the acceptance, disregard and cancellation of rides by the Uber driver, Uber tracks the percentage of rides cancelled by a driver. [Confidential].¹² Upon completion of the ride, the passenger (customer) is asked to rate the driver on a scale of 1 to 5. An average score below the threshold could (previously) lead to exclusion from the platform.

12. With the ride request, the driver receives information about the type of ride being requested (Uber X, Uber Green, etc.), the passenger's name, user rating, pickup location (including distance from the driver), destination location and estimated ride duration. In addition, the Uber driver can contact the passenger via text or phone. In turn, the passenger can request a certain type of ride from one location to another and receives a quote for the ride. After agreeing to the ride price, information about the driver who accepted the ride is displayed to the passenger. This information includes, but is not limited to, the driver's photo, name, rating, type of ride the driver is providing, live location, type of car, license plate number, and any messages and/or phone calls made by the driver.
13. Uber further assigns different classifications to Uber drivers, such as Gold, Platinum or Diamond. Based on the classification, a driver gets certain privileges on rides that can be profitable.¹³ To achieve a particular classification, a driver must meet the following criteria: 1) a rating of 4.85 out of 5; 2) an acceptance rate of 85% or higher, and 3) a cancellation rate of 4% or lower. In addition, Uber has a point system that allows a driver to earn points that factor into the rating.¹⁴
14. Differences of opinion between a passenger and a driver, for example about the fare, are handled by Uber. In such a case, Uber can unilaterally decide to refund the fare (in whole or in part) to the passenger, after which the driver is paid a lower amount for the ride.¹⁵

⁹ General Terms of Use of Uber, available at: <https://www.uber.com/legal/nl/document/?name=general-terms-of-use&country=netherlands&lang=en>, section 5.3 et seq.

¹⁰ File 4 and "Terms and Conditions for Independent Uber Partners," updated July 12, 2020.

¹¹ General Terms of Use of Uber, available at: <https://www.uber.com/legal/nl/document/?name=general-terms-of-use&country=netherlands&lang=en>, section 16.1.

¹² [confidential]

¹³ Ibid.

¹⁴ Ibid, r.o. 1.17.

¹⁵ Ibid, r.o. 1.16.



Date

July 22,

Our

reference

15. Finally, Uber may unilaterally decide to deny an Uber driver access to the Uber platform. The reasons for access denial include, for example, non-compliance, fraud, unacceptable behavior or dangerous driving. However, an average rating below 4.5 out of 5 could (previously) also lead to exclusion from the platform.¹⁶

2.3 The processing activities

16. Uber operates a centralized IT infrastructure on UTI's platform and servers located in the United States. Personal data of Uber drivers, located in the EEA, is therefore processed in the United States. In its investigation, the AP identified the following two relevant situations in which processing operations qualify as transfers within the meaning of the GDPR.
17. In the first situation, through the driver app, personal data of Uber drivers located within the EEA is collected and stored on a platform physically located in the United States.¹⁷ In addition to account and location data (depending on a country's legal rules), other data is also stored in the United States, such as ID, criminal and health data, and a cab license.¹⁸
18. The second situation concerns the exercise of GDPR rights by data subjects. UBV is responsible for assessing the scope of requests regarding data subjects' rights and for communicating with data subjects.¹⁹ UTI is responsible for making the personal data available to UBV in order to respond to requests from data subjects. According to the AP, there is a structural exchange of personal data between UBV in the Netherlands and UTI in the United States. First, through the driver app and by mail (from the device in the EEA), Uber drivers' personal data, processed within the EEA under the responsibility of UBV, ends up on UTI's servers in the United States. Second, there is a structural exchange of personal data between UBV and UTI.
19. The above situations are detailed by Uber as follows.²⁰
- Situation 1*
20. The first situation relates to the driver app within which Uber drivers in the EEA share personal data with UTI via their smartphone. When the driver first uses the app, the

¹⁶ Ibid, r.o. 1.13.

¹⁷ See file 11, Response to Request for Information 1, Attachment International Data Flows section, page 2. See also file 17, Response to Request for Information 2, Attachment UBV-UTI Data Sharing Agreement, page 2 et seq.

¹⁸ See File 23, Driver Requirements and File 17, Response to Request for Information 2, Appendix 2012UBV ROPA.

See also file document 17, Response to Intelligence Request 2, Appendix 2012UBV ROPA, page 2. The document discusses, among other things "evidence of health or fitness to provide services".

¹⁹ See File Exhibit 17, Response to Request for Information 2, Appendix UBV-UTI Data Sharing Agreement, pages 2 and 3, "UBV shall be responsible for assessing the validity and the scope of requests for the exercise of data subject rights, and for responding to the data subjects."

²⁰ See "Views of Uber on Investigation Report and Intent to Enforce," June 9, 2023, pp. 19-26.

AUTORITEIT
PERSOONSgegevens

Date

July 22,

Our

reference

the driver is asked to provide personal data such as his name, e-mail address and telephone number. The data is then stored on UTI's servers in the United States. Uber indicates that in this situation the driver provides his personal data directly to UTI without (technical) intervention of UBV or other European subsidiaries. This is confirmed in, among other things, the agreement between UTI and Uber B.V. on the responsibilities of both parties and other documentation provided by Uber.²¹

Situation 2

21. The second situation relates to the rights of data subjects. Specifically, 1) the assessment of the scope of data subjects' request regarding their rights under the GDPR, and 2) communication with data subjects regarding the exercise of their rights.
22. According to Uber, data traffic occurs from the moment the Uber driver makes a request (regarding their rights under the GDPR) until the moment Uber responds to the data subject's request. Uber further states that the data traffic between the data subject, UBV and UTI depends on the specific request made by a driver. Uber then provides a description of the standard procedures used in handling a data subject's request.
23. According to Uber, the first step in such a procedure is how the individual makes the request. Uber allows drivers to exercise their rights by:
 - a) filling out the form in the driver app or on Uber's website;
 - b) sending an e-mail to Uber; or
 - c) using other forms of communication (through a letter addressed to Uber or in a telephone conversation with an Uber employee).

Re (a)

24. Uber's driver app and website use UTI's servers located in the United States. Where an Uber driver wishes to exercise their rights under the GDPR directly through the driver app or Uber's website, the data flow associated with the processing of such requests will pass (directly) through the Uber driver's smartphone or other device located in the EEA, to UTI's servers located in the United States. This is regardless of which entity the data subject chooses to address. Uber states that at this stage, UTI is the only entity receiving the request, as the request is made to Uber's platform operated and managed by UTI.

Re (b)

25. An Uber driver may choose to exercise his rights by sending an e-mail to an address within the uber.com domain (e-mail address ending in uber.com). Uber's email traffic uses

²¹ See File No. 17, Response to Intelligence Request 2, Aug. 9, 2021, page 16 et seq. and Appendix UBV-UTI Data Sharing Agreement, page 2 et seq.

AUTORITEIT
PERSOONSgegevens

Date

July 22,

Our

reference

UTI's IT systems located in the territory of the United States. Uber states that in this situation there is only data traffic directly between the data subject (via his personal device) on EEA territory, to UTI's systems located in the United States.

Ad (c)

26. Uber drivers may choose to exercise their rights under the GDPR in other ways, such as by mail or telephone. Uber indicates that these other ways represent only a small percentage of the requests made by Uber drivers in the European Union (less than 10 requests per year). According to Uber, if the Uber driver chooses to send a letter to UTI's address in the United States or if the Uber driver telephones an employee in the United States and expresses his desire to exercise his rights, there is still direct data traffic from the driver located in the EEA to UTI in the United States.
27. According to Uber, if the Uber driver chooses to send his request to UBV located in the EEA or another subsidiary located in EEA territory, there is direct data traffic between the driver and that entity. Uber reaches the same conclusion if the Uber driver chooses to communicate by phone with an employee of Uber located in the EEA. After receiving the request, the employee advises the Uber driver to make his request in the driver app because the request can be handled most quickly through this route. If the Uber driver chooses not to do this, the employee puts a note directly into UTI's IT systems. Although these are located in the United States, the Uber employee (who is in EEA territory) can access them remotely.
28. In the case of letters, these are forwarded by UBV to UTI. Forwarding the letter and making a note (of a phone call made) is handled digitally by the UBV employee. The UBV employee connects via the browser on his computer to the Bliss Content system that uses UTI's servers in the United States. The content of the request made by the driver is described by the employee in this system. Uber indicates that this situation involves data traffic from the computer located in the EEA to the systems in the United States.
29. To further explain the data being processed, Uber states that an Uber driver who exercises a right through the driver app or website does not need to enter their personal data on the platform. Most Uber drivers are logged into the platform through their personal account. The data traffic that occurs when the request is made then consists of the specific request made by the driver (the data being requested) and the 'Universally Unique Identifier' (UUID) associated with the Uber driver's account. Each account on the Uber platform is associated with a UUID that identifies the Uber driver on the platform and Uber's systems.

AUTORITEIT
PERSOONSGEGEVENS

Date

July 22,

Our

reference

30. If the Uber driver is not logged into the platform (driver app or website), then a request can be made on the driver app or website by providing information regarding the rights to be exercised, the name, email address and phone number associated with the Uber driver's account. This information is necessary to link the request to the driver's UUID and initiate the process to process the driver's request. If the Uber driver makes the request by email, mail or phone, the driver will be asked for the same type of information.
31. The second step in the procedure is the preparation process to respond to the data subject's request. Most data subject requests are handled automatically through the self-service portal that the Uber driver has access to. The self-service environment is located on UTI's servers in the United States and has two functions: 1) 'Explore Your Data' which allows the Uber driver to view their personal data and 2) 'Download Your Data' which allows an Uber driver to download a copy of their personal data. If the request can be handled entirely through these functions in the self-service environment, then all necessary personal data is automatically collected in UTI's systems in the United States. This data is then shared directly with the data subject without any intervention by an Uber employee. With this fully automated preparation, Uber claims that there is no data movement from the EEA to the United States.
32. When the self-service environment cannot handle the request for reasons of query or complexity, an Uber employee must prepare the response to the driver's request (in part) manually. Uber notes that in the first four months of 2023, about 25 requests per month were handled this way.
33. In the process of partially manual response to the request, an employee of UBV must be able to view the data subject's request. The employee does this by accessing, through the browser of his/her computer located in the EEA, UTI's systems located in the United States. Uber indicates that this situation involves data traffic from the United States into the EEA, which includes the UUID number and the content of the driver's request.
34. Uber states that depending on the type of request made by the data subject, what type of personal data must be collected from the Uber driver to respond to the request. Because Uber has a centralized IT infrastructure on its platform and servers which are located in the United States, the personal data of Uber drivers located in the EEA are processed in the United States. To comply with the request, the employee must collect data located on UTI's servers. To collect the relevant personal data on the servers, the UBV employee must assess the scope of the data subject's request. Once the scope has been determined, the UBV employee accesses UTI's relevant systems via the browser on his/her computer located in the EEA. The scope of the data subject's request.
- parameters indicating the nature of the personal data - are entered into the search engine along with the UUID of the Uber driver by the relevant employee. In the systems of UTI

AUTORITEIT
PERSOONSgegevens

Date

July 22,

Our

reference

is then searched for the personal data that meet the criteria entered by the UBV employee in the search engine. This process takes place in its entirety on servers located in the United States, and it takes several hours before the results of the search are transferred directly to a spreadsheet on the server in the United States. After the information is transferred to the spreadsheet, the employee receives a message that the requested information is ready. The UBV employee can then view the spreadsheet through the browser of his/her computer in the EEA.

35. The UBV employee reviews the information collected and removes information that is outside the scope of the driver's request. If the data collected does not provide the information that can be used to adequately answer the request, the employee conducts a new search using the procedure described earlier. This procedure is repeated until the employee has the necessary personal information to adequately answer the request. Uber notes that the employee in question does not add personal information to the spreadsheet itself.
36. Uber indicates that data collection involves almost exclusively data traffic within the United States. It further notes that the UBV employee only has access to the personal data stored on UTI's servers in the United States. Uber expressly notes that the UBV employee thus has remote access to the personal data and that it will not be located on the UBV employee's server or computer located in the EEA territory. Only the entering of the parameters for selection is classified by Uber as data traffic from the EEA to the United States.
37. The final step in the (partially manual) process of handling data subjects' rights is responding to the request made by the driver. Once the aforementioned spreadsheet is populated with the personal data within the scope of the request, the spreadsheet is ready to be shared with the Uber driver. This step is performed by the UBV employee who, from the browser on his computer, has access to the spreadsheet and UTI's systems located in the United States. The employee in question instructs the system to export the spreadsheet to the so-called *"file mailbox"*. The data traffic associated with this process involves only data flow in the territory of the United States. Uber further explains this with that the *'file mailbox'* resides on UTI's servers and the spreadsheet residing on UTI's servers is exported from one system to another (but remains on UTI's server). Once the data is transmitted to the *'file mailbox,'* it is opened by the UBV employee and the employee then makes it available to the Uber driver. More specifically, the *'file mailbox'* sends a link to the Uber driver in the EEA and the Uber driver can use the link to download the personal data contained in the spreadsheet. According to Uber, this involves data traffic from the United States to the driver in Europe.
38. Uber notes that there is a temporary exception to this process when it comes to data subject rights regarding payment receipts. If a receipt is part of a driver's request for review, the UBV employee must retrieve the receipt from the UTI servers

AUTORITEIT
PERSOONSgegevens

Date

July 22,

Our

reference

to his computer located in the EEA. This document is then manually uploaded again by the UBV employee to the *"file mailbox"* on the servers in the United States.

After this document is uploaded, the UBV employee deletes the document from their computer. The data traffic this involves is a transfer of personal data from the United States to the EEA and back to the United States. Uber notes that this way of handling receipts is temporary and that they expect this process to be aligned with the procedure described above with respect to handling requests from data subjects within a few weeks.

2.4 Number of Uber drivers and GDPR requests from data subjects

39. The AP asked Uber about the number of registered Uber drivers in the EU and how often data subjects invoked their GDPR rights.
40. From August 6, 2021 to mid-February 2023, there were on average [confidential] drivers active in France and [confidential] drivers throughout the EU. As of Feb. 17, 2023, there were a total of [confidential] active drivers in the EU.²²
41. Uber conducted inspection requests of EU drivers between August 2021 and February 2023, [confidential] using the automatic *'download your data tool'*. This allows drivers to download their personal data based on the generic categories offered by Uber in the *'download your data tool'*. Uber has also carried out [confidential] deletion requests for (former) EU drivers. In addition, Uber states: *"in addition to using the 'Download Your Data' tool, between August 6, 2021 and February 1, 2023, Uber has processed [confidential] requests from French (former) drivers for an expanded access request."*²³

2.5 Uber's application of a transfertool

42. Uber has stated the following about the transfer of personal data to third countries:
*"For transfers of data subjects' data to third countries, Uber's standard practice is (and has been) to have standard contractual clauses (SCCs) in place when a third country has not been afforded an adequacy decision in order to ensure a high level of protection, and to conduct a 'third party risk management' assessment to identify potential risks and ensure data protection for its user's data."*²⁴
43. However, in 2021, Uber decided that standard contractual clauses are not necessary for processing personal data of EU drivers in the United States. Indeed, Uber argues that there is no onward transfer and that due to the joint responsibility of UBV and UTI, Article 3 of the GDPR is fully applicable to personal data processed in the United States.

²² See File 26, Response to Intelligence Request 4, March 13, 2023. The AP asked Uber for the number of registered drivers in the EU. The AP provided a number of reference dates for this to get an impression of the number of drivers over a period of time. To this, Uber provided the figures of drivers who had performed at least one ride in the 28 days prior to a reference date.

²³ See File Exhibit 30, Supplemental Responses from Uber March 23, 2023.

²⁴ See File No. 17, Response to Intelligence Request 2, Aug. 9, 2021, page 6.



Date

July 22,

Our

reference

Citing the European Commission's updated SCCs²⁵, Uber states the following: *"In light of this, Uber revisited its joint controller agreement to delete the SCCs, and to clarify joint controller responsibilities. Therefore, Uber has adopted a new version of its joint controller agreement, in which the new regulatory requirements and relationship between UTI and UBV are reflected"*.²⁶

44. The Data Sharing Agreement to which Uber refers has a version date of Aug. 6, 2021. Thus, based on Uber's statement, the AP finds that as of Aug. 6, 2021, Uber removed the standard contractual provisions for the transfer of personal data to third countries from the aforementioned agreement.²⁷ Uber had also not implemented other transfer instruments, such as binding business rules or a certification mechanism, thereafter.²⁸
45. On July 10, 2023, the European Commission adopted the adequacy decision "EU-U.S. Data Privacy Framework".²⁹ Uber certified itself under the EU - US Data Privacy Framework on November 27, 2023.³⁰ Uber says the following in its privacy statement :³¹

"When we transfer user data from the EEA, UK and Switzerland, we do so on the basis of the necessity to fulfill our agreements with users, consent, adequacy decisions regarding the country of transfer (available [here](#), [here](#) or [here](#)), and transfer mechanisms such as the Standard Contractual Clauses adopted by the European Commission (and their approved equivalents for the UK and Switzerland), and the EU-U.S. Data Privacy Framework ("EU-U.S. DPF"), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework ("Swiss-U.S. DPF"), as set forth by the U.S. Department of Commerce. [...] UTI has certified to the United States Department of Commerce that it adheres to (1) the EU-U.S. Data Privacy Framework Principles regarding the processing of personal data received from EEA member countries in reliance on the EU-U.S. DPF [...] In the event that the EU-U.S. DPF or the Swiss-U.S. DPF are invalidated, Uber will transfer data that is subject to these certifications in reliance on the other data transfer mechanisms described above."

3. Views Uber

46. The AP believes that Uber violated Article 44 of the GDPR because Uber allowed transfers of personal data to the United States from August 6, 2021 to November 27, 2023 while there was no valid adequacy decision and appropriate safeguards were not provided as stipulated in Chapter V of the GDPR. The AP summarizes Uber's views in Chapter 3. Chapter 4 follows the AP's legal rationale for the breach and also follows the AP's response to Uber's views.

Application of chapter V GDPR

²⁵ European Commission Implementing Decision (eu) 2021/914.

²⁶ See File No. 17, Response to Intelligence Request 2, Aug. 9, 2021, page 5.

²⁷ See file document 17 Response to Intelligence Request 2, Attachment UBV-UTI Data Sharing Agreement.

²⁸ See Articles 46 and 47 GDPR for a complete overview.

²⁹ https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en

³⁰ <https://www.dataprivacyframework.gov/list>

³¹ <https://www.uber.com/legal/nl/document/?name=privacy-notice&country=france&lang=en>



Date

July 22,

Our

reference

47. Uber believes that Article 44 GDPR has not been violated because Chapter V of the GDPR does not apply to the processing operations under investigation. First, according to Uber, Chapter V does not apply because Article 3 GDPR already applies. Chapter V, according to Uber, is intended to catch cases that fall outside the scope of Article 3 GDPR, lest the protection offered by the GDPR be undermined. Since the application of Article 3 GDPR already protects the data, simultaneous application of Article 3 GDPR and Chapter V GDPR is duplicative and thus meaningless.
48. Second, Uber argues that Chapter V is subordinate to Article 3, and therefore cannot be applied simultaneously. Any other interpretation, according to Uber, is contrary to international commitments of the EU, in particular the WTO Agreement and its accompanying GATS agreement. It follows from these international commitments that member states may not treat non-European entities more unfavorably than European entities under the agreement. Case law has established that secondary Community law, including the GDPR, should be interpreted as much as possible in line with international law. A simultaneous application of Article 3 GDPR and Chapter V is contrary to EU obligations under international law and the obligation to interpret secondary Community law in line with international law. Therefore, the relationship between Article 3 GDPR and Chapter V GDPR should be interpreted in such a way that they cannot apply simultaneously.
- The concept of 'transfer'*
49. Uber argues that the concept of "transfer" is not defined by the GDPR. This was a deliberate choice of the European legislator who did so despite the objections and opinions of various institutions such as the EDPS, the EEC and the EDPB. In addition, European data protection authorities, including the AP, never fleshed out the concept until February 14, 2023 despite being requested to do so by various stakeholders. Only on Feb. 14, 2023, did the EDPB come up with an interpretation of the concept of "transfer," but in addition to the fact that it itself admits that it is a legally uncertain concept because the GDPR does not define it, the EDPB's own interpretation is only one possible interpretation and, moreover, non-binding. In addition, the EDPB has asked the EC to further clarify the concept. For the above reasons, the AP cannot rely on this single interpretation without further substantiation.
- No transit in the present case*
50. Uber further argues that there is no transfer because, according to the EDPB guidelines, there must be a processor or controller acting as an exporter of the personal data while in this case it concerns data subjects who themselves make the personal data directly available to UTI. Insofar as it is argued that Uber exports the data because the drivers do so under the responsibility of UB, this argument does not succeed, because the AP thereby introduces a new standard that does not follow from the guidelines nor from the GDPR. Furthermore, the argument does not succeed because 1) the actual data transfer must be assessed, 2) it does not follow from the qualification as joint controllers that UB itself makes the personal data available, and 3) it also does not follow from the factual and legal division of responsibilities between UB and UTI that UB is responsible for sharing personal data to UTI when a driver does so.



Date

July 22,

Our

reference

Transfer instruments and grounds for exception

51. Uber argues that even if there were transfers, these transfers are in compliance with Chapter V GDPR. First, Uber implemented standard contractual clauses in the Data Sharing Agreement (DSA) between joint controllers UBV and UTI until August 6, 2021 as an unobligatory safeguard for the data transfers under investigation. Uber removed the standard contractual clauses from it in good faith because on June 4, 2021, with the introduction of new standard contractual clauses, the EC stated in the recitals that the new standard contractual clauses should not be used to the extent that the importer's processing falls within the scope of Art. 3(2) GDPR. Also, the lack of any progress by the EC in developing standard contractual clauses specifically for importers that already fall within the scope of the GDPR shows that the EC has so far taken the position that application of Art. 3 GDPR excludes application of Chapter V GDPR. In any case, according to Uber, it is established that no standard contractual clauses were available to Uber in the interim. Besides the standard contractual clauses, according to Uber, all alternative transfer instruments are currently not realistic alternatives.
52. Second, any transfer of personal data by Uber is lawful because Uber believes that it can rely on the exception of Art. 49(1)(b) and (c) GDPR. Uber argues that transfer based on Art. 49 GDPR does not require that the level of protection in the third country is broadly equivalent to the level of protection guaranteed within the EU by the GDPR. Merely complying with the conditions mentioned in Art. 49 GDPR is sufficient, according to Uber. This follows, among other things, from the wording of the GDPR and from *Schrems II* paragraph 202 of law.
53. In any case, according to Uber, both grounds for exemption do not require, as the AP argues, that the transfer be "incidental." Although this does follow from recital 111 to the GDPR, this is at odds with the text of the GDPR itself, the case law of the CJEU and the central government's manual. First, "incidental" is not in the text of the GDPR. Indeed, it says that Article 49 can also be used for a *series of* transfers. Second, recitals to the GDPR do not create a new standard and have no independent legal force, as also confirmed by standard case law of the CJEU, among others. Third, judges do not use "incidental" as a condition, and, on the contrary, Article 49 should be interpreted broadly in the case of data transfers within companies or among a group of companies. Fourth, the manual of the Ministry of Justice and Security does not mention 'incidental' as a condition. In addition, grounds b and c do require that the transfer is necessary, but, according to Dutch case law, this necessity need not be narrow and substantial.
54. Uber argues that if international transfer is assumed, it can rely on Article 49(1)(c) for the situation where drivers make GDPR requests and on Article 49(1)(b) for cases where drivers use the driver app.
55. As for the situation where GDPR requests are made by drivers, this transfer meets all the conditions of Art. 49 (1) (c) GDPR. In particular, because the transfer



Date

July 22,

Our

reference

is necessary for the conclusion or performance of contract concluded in the data subject's interest between the controller and another natural or legal person. The agreement is concluded in the interest of the data subject because the DSA regulates and facilitates the GDPR rights that constitute and support the data protection of the drivers, this also follows from Art. 26 GDPR and the accompanying Recital 79. The transfer is further necessary for the performance of the contract. Indeed, the transfer takes place within the framework of the DSA and is directly related to the completion of inspection requests. In addition, the data transfer is unavoidable due to Uber's centralized IT infrastructure, which in turn is crucial for Uber's specific services as well as for the global application of Uber's technical and organizational GDPR measures. Finally, according to Uber, there are very few data transfers in the context of access requests (only 25 per month).

56. As for the situation where drivers use the driver app, the transfer meets all the conditions of Art. 49(1)(b), and in particular the condition that there is a transfer necessary for the performance of an agreement between the data subject and the data controller (UBV and UTI through the DSA). The necessity, according to Uber, follows from being able to fulfill the agreement between UBV and the driver. Uber must fulfill its contractual obligation to offer rides, and can only do so based on data transfer from the driver (e.g., his location). The data transfer is thus necessary to execute the contract between the driver and Uber.

4. Review

4.1 Processing of personal data

57. The AP comes to the following assessment. The use of the driver app requires drivers to create an account. The documents and personal information collected during this registration allows Uber to start its processing activities of personal data of Uber drivers.
58. The AP found in section 2.3 that Uber processes various data from Uber drivers in that context. In addition to account data, location data, photos, payment receipts and ratings, Uber also processes (depending on the legal rules in a country) other data, such as ID, criminal and health data.
59. The AP considers that Uber thus processes personal data as referred to in Article 4(1) and (2) of the GDPR.

4.2 Controller and authority AP



Date

July 22,

Our

reference

60. Uber B.V. is a company based in the Netherlands and is part of the Uber group of companies. Uber Technologies Inc. is based in the United States and is the parent company of, among others, Uber B.V. The (French) drivers entered into an agreement with Uber B.V.
61. The concepts of "controller" and "processor" are functional concepts: they are intended to allocate responsibilities according to the actual role of the parties, which means that the legal status of a party as a "controller" or as a "processor" should in principle be determined by its actual activities in a specific situation, and not by the formal designation of a party as a "controller" or "processor" (e.g., in a contract).³²
62. Uber B.V. and Uber Technologies Inc. jointly determine the purposes and means of processing for Uber drivers' personal data in the European Economic Area (EEA). The AP therefore believes that UBv and UTI should be considered joint controllers for the international transfer that is part of two larger sets of processing activities as described in situations 1 and 2. Joint processing responsibility has not been disputed by Uber. For requests related to data subjects' rights (situation 2), the division is that UBv is responsible for assessing such requests and that UTI provides the technical means and personal data. UTI is also the publisher of the driver app.
63. The AP further notes that the processing of personal data of Uber's drivers involves the processing of data in the course of the activities of an establishment of a controller or processor in the Union, as provided in Article 3(1) of the GDPR.
64. Finally, Uber offers its services in multiple EU member states and for these services Uber processes personal data. This means that data subjects in more than one Member State are substantially affected by Uber's processing of personal data. This amounts to cross-border processing (Article 4, introductory paragraph and 23 (a) and (b) of the GDPR). The AP notes that Uber's central administration in the EEA is located at Uber B.V. Therefore, Uber B.V. is considered a principal place of business within the meaning of Article 4(16) GDPR. In view of this, the AP is competent to act as lead supervisory authority within the meaning of Article 56(1) GDPR.

4.3 Territorial scope and chapter V GDPR

65. Uber believes that Article 3 GDPR and Chapter V GDPR cannot apply simultaneously.³³

³² See EDPB Guidelines 07/2020 on the terms "controller" and "processor" in the GDPR, pp. 3 and 10.

³³ See "Views of Uber on Investigation Report and Intent to Enforce," June 9, 2023, Section 6.2.2, pp. 28-31.



Date

July 22,

Our

reference

66. The AP notes that the rationale of data transfer under Chapter V GDPR, is complementary to the rationale of the territorial scope of the GDPR as laid down in Article 3. Namely, to prevent the denial, undermining or circumvention of data protection provided by EU law.³⁴ By making EU law applicable to processing operations taking place outside the borders of the EEA, Article 3 GDPR aims to ensure the high level of data protection guaranteed by the GDPR.³⁵ The provisions in Chapter V GDPR on transfer achieve this by requiring the application of EU standards-based protection to such processing operations.³⁶ It should be noted that although the GDPR applies to all processing operations under Article 3 GDPR, the application of the GDPR outside the EEA territory does not provide the same protection. Indeed, the application of the GDPR in the Union is based on the legal framework of EU law in areas such as the recognition and enforcement of judgments/rulings, the rule of law, the independence of the judiciary and Data Protection Authorities, and other basic areas which by their nature do not apply to third countries.³⁷ In several rulings related to international data transfers, the CJEU expresses this concern by assessing whether personal data have been processed in a way that meets EU standards.³⁸ The AP therefore notes that the provisions in Chapter V contain mechanisms, which counterbalance the difficulty of enforcing obligations under EU law against parties in third countries. The AP believes that any other interpretation of these mechanisms would lead to a weakening of the protection offered within the Union, which is not consistent with the standard required by the CJEU.³⁹
67. To further explain the above, the AP notes that within the jurisdiction of the United States, it is difficult to enforce compliance with the GDPR against foreign companies including Uber. To counterbalance this, the data transfer provisions in Chapter V GDPR place a direct obligation on parties processing data in third countries by requiring them to comply with the standards of the GDPR.
68. With respect to Uber's argument that Article 3 GDPR prevails over Chapter V, or the argument not to apply provisions of Chapter V when Article 3 GDPR applies, the AP notes

³⁴ Concepts in data protection should be interpreted broadly so that no one is deprived of full and adequate protection. This view is expressed by the CJEU in judgments regarding international data processing indicating the need to ensure a consistent and uniform application of the Charter and to prevent the circumvention of protection. See in that regard C-311/18, *Schrems II*, ECLI:EU:C:2020:559, para. 101 and C-131/12, *Google v Spain*, ECLI:EU:C:2014:317, para. 54 and 58.

³⁵ Recital 23 of the GDPR.

³⁶ C-362/14, *Schrems*, ECLI:EU:C:2015:650, para. 73.

³⁷ For example, Article 36 GDPR requires prior consultation with the relevant Data Protection Authority in those cases where data processing would result in a high risk. However, there are no provisions in the GDPR by which a competent Data Protection Authority for a data processing outside the Union can be identified.

³⁸ C-362/14, *Schrems*, ECLI:EU:C:2015:650, at 90, Conclusion 1/15, *EU Canada PNR Agreement*, ECLI:EU:C:2017:592, at 212-215 and C-311/18, *Schrems II*, ECLI:EU:C:2020:559, para. 184. Regarding the ECJ's view that Data Transfer 'must ensure a high level of protection essentially equivalent to that under EU law' in C-101/01, *Bodil Lindqvist*, EU:C:2003:596.

³⁹ See in that context, for example, C-40/17, *Fashion ID GmbH c Co. KG*, ECLI:EU:C:2019:629, para. 50.



Date

July 22,

Our

reference

that any variation on the interpretation described would conflict with the status Chapter V has within the structure of the GDPR. Article 44 GDPR makes the connection between Chapter V and the other provisions by providing that transfers of personal data may only take place if all other relevant provisions of the GDPR are met.⁴⁰ The CJEU confirmed this view by stating that the transfer of personal data to a third country is a processing operation that falls within the scope of the GDPR and that where the GDPR applies, the provisions relating to data transfers should also apply.⁴¹ Furthermore, the European Data Protection Board (hereinafter EDPB) states that the application of the GDPR entails that all the provisions of the GDPR apply to processing operations that fall within the territorial scope of the GDPR.⁴² Including the obligations set forth in Chapter V of the GDPR.

69. The AP notes that there are important differences between Article 3 GDPR and Chapter V GDPR and emphatically states that Article 3 GDPR does not take precedence over Chapter V. Moreover, there are consequences for not applying Chapter V GDPR. The territorial scope set forth in Article 3(1) of the GDPR means that the regulation applies to processing of personal data in the context of activities of an establishment of a controller or processor in the Union, regardless of whether the processing takes place in the Union. Thus, the GDPR applies even if the processing does not technically take place in the Union, but is bound by the GDPR through a continuing relationship with a permanent establishment in the Union (such as a branch, or subsidiary). Such a relationship is fairly readily assumed, for example, if the establishment in the Union generates revenue for the parent entity in the third country. Such is certainly the case between Uber B.V. and UTI in the present case. By contrast, the data transfer provisions set forth in Section V address the specific context of transfers of personal data to a third country entity by a processor or data controller, where the exporter of the personal data must implement appropriate safeguards so that the personal data enjoys an equivalent level of protection as the GDPR provides within the Union. This protection is thus complementary to Article 3 GDPR. This complementary set of provisions of the GDPR set a high standard of protection both in practice and by law to prevent circumvention of the protection provided by EU law.⁴³
70. Finally, with respect to the relationship between Article 3 GDPR and Chapter V GDPR, Uber argues that the GDPR (being secondary Union law) must be interpreted in accordance with international agreements, in this case the WTO agreements.

⁴⁰ Article 44 GDPR states that data may be transferred only if the conditions set forth in Chapter V are met, which entails ensuring compliance before the transfer takes place.

⁴¹ C-311/18, *Schrems II*, ECLI:EU:C:2020:559, para. 83.

⁴² EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), p. 5.

⁴³ The CJEU noted in its rulings that the GDPR must provide sufficient protection, both in law and in practice, see C-362/14, *Schrems*, ECLI:EU:C:2015:650, r.o. 64-65 and 95, Conclusion 1/15, *EU Canada PNR Agreement*, ECLI:EU:C:2017:592, margin 220. C-311/18, *Schrems II*, ECLI:EU:C:2020:559, paragraphs 105 and 187.

AUTORITEIT
PERSOONSgegevens

Date

July 22,

Our

reference

71. Uber first notes that the European Union, and each of its member states, is a party to the Marrakesh Agreement Establishing the World Trade Organization (WTO Agreement)⁴⁴ and the annexes to the WTO Agreement (including the GATS Agreement).⁴⁵ It follows from these international agreements that non-European entities, such as UTI, may not be treated more adversely than European entities by participating states. Since, according to Uber, a simultaneous application of both the obligations of the GDPR based on Article 3 GDPR and Chapter V GDPR is more disadvantageous to UTI as a non-European entity, Uber considers that both systems cannot be of simultaneous application. In conclusion, the AP's interpretation, namely that Chapter V and Article 3 GDPR can be applied simultaneously, is contrary to EU international obligations, according to Uber.
72. While the AP will not dispute that the GDPR should in principle be interpreted as much as possible in accordance with international agreements, it must note that Uber's argument misses the fact that case law has already established that two cumulative conditions do need to be met for the interpretation advocated by Uber, namely:
1. The nature and design of that agreement (the WTO Agreement in this case) do not preclude an action for annulment or plea of illegality of (secondary) Union law (the GDPR);
 2. The provision (the WTO Agreement) is sufficiently unconditional in content and sufficiently precise to trigger an action for annulment or plea of illegality of secondary Union law (the GDPR).⁴⁶
73. It follows from settled case law that the WTO Agreement does not satisfy at least the first requirement. Its nature and design preclude the WTO Agreement from taking precedence over the GDPR. It also resists the proposition that the WTO Agreement is leading for the interpretation of secondary Union law (such as the GDPR).⁴⁷ Thus, also in this context, the AP maintains its position that Article 3 GDPR (and all obligations that follow therefrom) and Chapter V GDPR apply simultaneously in this case.
74. In addition, paragraph 3 of the introduction to the annexed schedule referred to by Uber in its written submission⁴⁸ states in so many words that the rights and obligations arising under the GATS, including the schedule of commitments, do not have direct effect, "*so as not to confer any direct rights on individuals natural or legal persons.*" Thus, Uber cannot invoke WTO agreement and related GATS commitments in the present case.

4.4 Is there any transfer of personal data?

⁴⁴ Marrakesh Agreement establishing the World Trade Organization, April 15, 1994.

⁴⁵ General Agreement on Trade in Services, April 15, 1994.

⁴⁶ See in particular judgment of Jan. 13, 2015, Council and Others v. Vereniging Milieudefensie and Stichting Stop Luchtverontreiniging Utrecht, C-401/12 P-C-403/12 P, EU:C:2015:4, at para. 54 and case law cited there.

⁴⁷ See in particular judgments of November 23, 1999, Portugal v. Council, C 149/96, EU:C:1999:574, para. 47; March 1, 2005, Van Parrys, C 377/02, EU:C:2005:121, para. 39, and February 4, 2016, C J Clark International and Puma, C 659/13 and C 34/14, EU:C:2016:74, para. 85.

⁴⁸ List of specific commitments of the European Union annexed to the General Agreement on Trade in Services (GATS) (OJEU 2019/C 278), p. 59.



Date

July 22,

Our

reference

4.4.1 Legal framework

75. Article 44 GDPR provides that *"personal data processed or intended for processing for transfer to a third country or an international organization may be transferred only if, without prejudice to the other provisions of this Regulation, the controller and processor have complied with the conditions laid down in this chapter; this also applies to further transfers of personal data from the third country or an international organization to a third country or another international organization. All the provisions of this Chapter shall be applied to ensure that the level of protection guaranteed by this Regulation for natural persons is not undermined."*
76. Furthermore, recital 101 GDPR notes *"[...] Where personal data are transferred by right of the Union to controllers, processors or other recipients in the same or a third country or in the same or another international organisation, this should not be to the detriment of the level of protection ensured to natural persons in the Union by this Regulation, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or a third country or in the same or another international organisation. [...] In any case, transfers to third countries and international organizations may only take place in full compliance with this Regulation. A transfer may take place only if the controller or processor, subject to the other provisions of this Regulation, complies with the provisions of this Regulation in relation to the transfer of personal data to third countries or international organizations."*
77. The GDPR does not define transfer'. However, in its Guidelines, the EDPB has identified three cumulative criteria that a transfer must meet:
1. A controller or processor ("exporter") is subject to the GDPR for the particular processing activity.
 2. Personal data that is the subject of such processing shall be provided by the exporter by transmission or otherwise made available to another controller, joint controller or processor ("importer").⁴⁹
 3. The importer is located in a third country (whether or not such importer is covered by the GDPR for the particular processing activity under Article 3) or is an international organization.⁵⁰
78. If the above criteria are met, there is a transfer and Chapter V GDPR applies. This means that the transfer may only take place under the conditions specified in an adequacy decision of the European Commission⁵¹ or by providing appropriate safeguards.⁵² If these are not met then the GDPR provides derogations (exceptions) for specific situations.⁵³

⁴⁹ See also EDPB Guidelines 07/2020 on the terms "controller" and "processor" in the GDPR.

⁵⁰ EDPB Guidance 05/2021 on the interaction between the application of Article 3 and the provisions on international transfers under Chapter V of the GDPR, p. 7.

⁵¹ Article 45 GDPR.

⁵² Article 46 GDPR.

⁵³ Article 49 GDPR.



Date

July 22,

Our

reference

79. In the present case, the AP assesses whether the processing operations described in situation 1 a 2 qualify as transfers of personal data where the provisions set out in Chapter V GDPR must be complied with.

4.4.2 Review

80. Regarding the first criterion, the AP finds that the processing meets the requirements of Article 3(1) GDPR, namely that a controller or processor is subject to the GDPR with respect to the processing in question.⁵⁴ This conclusion is acknowledged by Uber. More specifically, Uber has stated that UBV, with respect to its processing of Uber drivers' personal data in the EEA, is subject to the GDPR. And Uber further expressly states that both UBV and UTI are bound by the GDPR under Article 3(1) GDPR.
81. Regarding the second criterion, Uber argues that there is no transfer. Uber explains this by stating, *"Chapter V of the GDPR does not apply to certain aspects of Uber's business and the related international data flows cannot be considered international data transfers"* because UBV and UTI are joint controllers for whom the GDPR is directly applicable under Article 3(1) GDPR. Despite this reasoning, Uber nonetheless acknowledges data transfers between UBV and UTI. However, according to their written statements, they believe that these should not be classified as transfers because both UBV and UTI are subject to the GDPR.⁵⁵
82. The AP believes otherwise. As noted earlier, not applying Chapter V GDPR because UBV and UTI are directly subject to the GDPR would have the effect of undermining the high level of protection of the GDPR. Transfers can occur under different types of circumstances where entities are subject to the GDPR under Article 3 GDPR. Transfers between joint controllers subject to Article 3 can also take place and are not excluded from the GDPR's transfer provisions. This view is consistent with the EDPB's position as reflected in the second criterion for transfers: "Personal data that is the subject of such processing is provided or otherwise made available by the exporter to another controller, joint controller or processor ("importer") by means of transmission."
83. The ECJ requires data protection to be effective not only in law but also in practice. This includes having effective redress mechanisms and remedies against violations of the GDPR.⁵⁶ If the relevant processing is covered by the GDPR and the personal data is processed by an entity outside the Union, then the processing falls under legal frameworks that may conflict

⁵⁴ See also Section 4.2. and EDPB Guidance 3/2018 on the Territorial Scope of the GDPR (Article 3).

⁵⁵ File 11, Response to Intelligence Request 1, Appendix to International Data Flows, p. 6.

⁵⁶ See also EDPB Guidelines 3/2018 on the Territorial Scope of the GDPR (Article 3) and C-311/18; *Schrems II*, ECLI:EU:C:2020:559, r.o. 186- 189.



Date

July 22,

Our

reference

with or undermine the GDPR. Regulation of international transfers therefore counterbalances the difficulty of enforcing obligations under EU law against parties outside the Union.

84. According to the CJEU, the concept of data controller as laid down in Article 4, introductory wording and point 7 of the GDPR must be interpreted broadly in order to ensure effective and full protection of data subjects.⁵⁷ In the AP's view, this understanding should be applied analogously to the concept of "exporter. A restrictive interpretation of the 'exporter' criterion would mean that Uber drivers would not be effectively and fully protected because there would be no accountable exporter with responsibility for complying with obligations on the transfer of personal data outside the EEA. The exporter is the entity that must comply with the Chapter V transfer regulations and assess what appropriate safeguards are necessary to ensure an equivalent level of protection for personal data (as guaranteed under the GDPR). In addition, the data subject must be able to hold the controller accountable within the meaning of Article 5(2) jo. 44 GDPR.
85. Moreover, the ECJ requires that personal data originating in the Union must enjoy a high level of protection, even if they are processed in or transferred to third countries. Any interpretation or implementation of the provisions of Article 3 and Chapter V must meet that standard. Again, the AP believes that the concept of "exporter" in the second criterion as elaborated in the EDPB Guidelines should not be interpreted restrictively.
86. Also due to developments in law and jurisprudence, a restrictive interpretation is inconsistent with the goal of providing a high level of protection for personal data. From the moment the Charter of Fundamental Rights of the European Union (hereinafter: Charter) became primary law,⁵⁸ the CJEU has invoked the Charter to highlight the high level of protection for international transfers in the context of international agreements of the Union,⁵⁹ adequacy decisions of the Commission⁶⁰ and the Commission's Standard Contractual Clauses (SCCs).⁶¹ In light of these rulings, the AP views international transfers from the perspective that providing a high level of protection is the starting point and interprets the term "exporter" broadly.
87. In the present case, and considering the technical developments, the criterion of 'exporter' (a controller or processor in the EEA transferring personal data to a third country) deviates from the so-called classical model. To illustrate this, the AP notes that within the given context, extensive instructions are provided by Uber to the data subject - the Uber driver in the EEA - on how to provide specific personal data. Moreover, the Uber drivers are required to comply with conditions set by the Uber in advance with respect to under

⁵⁷ See, for example, C-210/16, *Unabhängiges Zentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein*, ECLI:EU:C:2017:796, at para. 28 and C-25/17, *Jehovah's witnesses*, ECLI:EU:C:2018:551, at para. 66.

⁵⁸ See also Article 6(1) TFEU.

⁵⁹ Conclusion 1/15, *EU Canada PNR Agreement*, ECLI:EU:C:2017:592, marginal 119-231.

⁶⁰ C-362/14, *Schrems*, ECLI:EU:C:2015:650, para. 38-40.

⁶¹ C-311/18, *Schrems II*, ECLI:EU:C:2020:559, para. 99.



Date

July 22,

Our

reference

other processing of their personal data in the context of a (pre)contractual employment relationship. Furthermore, Uber employees in the EEA, for example UBV employees, must comply with Uber's internal policies prescribing mediation between the Uber driver and UTI.⁶² Uber also explained that when an Uber driver has trouble, for example, taking the mandatory profile picture for the driver app, the Uber driver can go to a Greenlight Hub location in the EEA where an employee helps the Uber driver (on the spot) take a picture with the Uber driver's smartphone. The Uber driver can then upload the profile photo to the Uber IT platform managed by UTI with the employee's instruction. In this particular case, the personal data is technically transferred from the data subject's personal device from the EEA to the Uber platform operated by UTI and located in a third country. However, despite these Uber-initiated processing activities that occur prior to and during the contractual relationship between the Uber driver and UBV, Uber attributes the continuous transfer of personal data from the EEA to a third country to the data subject in Situations 1 and 2.

88. The AP notes that Uber drivers provide their personal data by entering it on the Uber platform and that it is collected by Uber through the Uber driver's personal device, within the EEA, and ends up on Uber's IT systems (managed by UTI) in the United States. This results in data traffic of personal data from the EEA to the United States. In AP's view, however, this in no way means that the data transfers by Uber, as it took place and continues to take place as described in Situations 1 and 2, do not involve transfers of personal data from UBV to UTI within the meaning of the GDPR.⁶³ Uber uses the driver app as a technical tool to transfer personal data from the EEA to the United States. UBV therefore shares responsibility and has (technical) control over the transfer of personal data from the EEA to the United States.
89. Furthermore, the AP believes that the question of whether there is international transfer should not be judged solely on the basis that it is the driver who operates the driver app via his private device. It must also be considered that Uber exerts a large degree of influence over the context in which those actions and the will of the driver come about. That context consists of various elements preconceived by Uber that effectively leaves the driver no choice but to enter the data into Uber's app. The following will explain what these elements are and how they determine the context in which the data transfers come about. It will become clear that the attribution of the transfer to the driver by Uber (which is only a link of minor significance in the whole process and context of the processing) undermines the protection provided by the GDPR for the processing of personal data.

⁶² An example of these policies was explained in more detail at the viewpoint hearing, see the minutes of the viewpoint hearing held on July 5, 2023.

⁶³ With the exception of the case where personal data is sent by Uber from the U.S. to the EEA in responding to requests of data subjects on the exercise of their GDPR rights.

AUTORITEIT
PERSOONSgegevens

Date

July 22,

Our

reference

90. First, the modern business model as well as the technical architecture of the platform and Uber's internal policies are designed to serve Uber's business purposes. In the present case, UBV, which enters into an agreement with Uber drivers (in EEA territory), is identified as the data controller initiating the collection of personal data through the Uber platform in a pre-contractual employment-related relationship. At this stage, the drivers provide their personal data through their personal device, within the EEA, on the driver app platform operated by UTI located outside the Union. From then on, Uber continuously collects and processes personal data through the Uber driver's personal device. Subsequently, the personal data of Uber drivers in the EEA is made accessible by transmission or otherwise to, and stored on, UTI's servers in the United States. The AP therefore finds that in the contractual relationship between Uber drivers within the EEA and UBV, UBV is the exporter of the personal data and UTI is the importer.
91. This view is consistent with "providing effective and complete protection" of personal data required by the CJEU. Furthermore, this interpretation does not conflict with the Guidelines.⁶⁴ The Guidelines provide several examples illustrating the situations in which a processing operation should be considered a transfer. However, an example of a situation like the one in the present case, more specifically an example of an 'exporter' in the context of a (pre)contractual employment-related relationship, is not given. In this case, the data subjects provide the personal data through their personal device on the platform operated by a third-country entity, UTI. The contractual relationship between Uber drivers in the EEA and UBV
- where the terms are unilaterally predetermined by Uber - allows Uber drivers in the EEA to access the Uber driver platform. The core business of providing transportation services on Uber's platform requires the Uber driver to upload personal data and Uber to continuously collect personal data from the Uber driver's device. The personal data is then processed for various purposes jointly defined by UBV and UTI, involving transfers from the EEA to the United States.
92. Moreover, the AP's view, which identifies UBV as the "exporter" and UTI as the "importer," is corroborated by the following details of the relationship between Uber drivers and Uber (UBV and UTI).
- The platform for Uber drivers is set up by Uber in such a way that the Uber driver must enter their personal data via their personal device on the platform in order to access the platform, schedule activities (i.e., information events), receive support and provide transportation services. Uber also stipulates that the personal data of EU drivers will be processed on UTI's platform in a third country. The little actual influence Uber drivers have over their personal data vis-à-vis data controllers is an important factor in qualifying UBV as an exporter in the present case;

⁶⁴ EDPB Guidance 05/2021 on the interaction between the application of Article 3 and the provisions on international transfers under Chapter V of the GDPR.



AUTORITEIT
PERSOONSgegevens

Date

July 22,

Our

reference

- Regarding the collection of personal data and/or otherwise processing of personal data of Uber drivers through the Uber platform by UBV and UTI, AP reiterates again that the purposes and means of processing personal data are determined unilaterally by UBV and UTI. If a data subject decides to become an Uber driver in the EU, this requires creating an account on the Uber platform⁶⁵ and then accepting the terms and conditions. By agreeing to the terms and conditions, the Uber driver enters into a contract with UBV which then subjects the Uber driver to the predetermined purposes and means of processing their personal data by UTI and UBV;
 - The AP expressly notes that although Uber drivers entered into the contract of their own free will, this does not automatically mean that they have any influence on determining the purposes and means of processing their own personal data. Especially since the terms and conditions that Uber drivers must accept are drafted in advance and are not negotiable. Furthermore, Uber exercises complete authority over the activities on the platform and the data processing that results from these activities. For example, Uber influences certain aspects of Uber drivers' behavior by providing financial incentives to perform more rides and by having passengers rate their Uber driver, which may result in the Uber driver being excluded from the platform.⁶⁶
93. Moreover, the AP found that Uber has control over Uber drivers' behavior and personal data through their platform in other ways, namely:
- Uber drivers are controlled by an algorithm of the driver app which is predetermined by Uber and through which Uber exercises control over data processing.⁶⁷ In addition, Uber sets certain requirements that an Uber driver must meet. To demonstrate compliance with these requirements, the Uber driver must upload documents containing personal data on the platform. For example, as an Uber driver, one must own a car. The vehicles allowed to be driven on behalf of Uber must meet certain conditions that seem to vary from country to country where Uber transportation services are provided. The vehicles must be approved and meet the condition of mandatory insurance. The driver must further hold a driver's license and must not have a criminal record. These documents are reviewed by UBV and UTI even before an Uber driver is given permission and/or authorization to accept rides in their neighborhood.
 - Based on driver quality and vehicle type, the transportation services offered by Uber are categorized.
- [confidential]

⁶⁵ The Uber driver's personal data is then entered on servers owned and operated by UTI. These servers are located in the United States where the personal data is further processed.

⁶⁶ Court of Amsterdam, ECLI:NL:RBAMS:2021:5029, r.o. 1.13.

⁶⁷ Ibid, r.o. 16-35.

AUTORITEIT
PERSOONSgegevens

Date

July 22,

Our

reference

[confidential]

[confidential]

[confidential]

The remaining amount is paid to the Uber driver.⁶⁸ In order to carry this out, the personal data of Uber drivers are processed by UTI and UBV.

- Uber allows passengers to access their platform and perform transportation services subject to terms and conditions imposed by Uber that are binding on drivers through an agreement for use of the platform. The terms cover the acceptance and pursuit of activities and even the behavior of drivers while providing the service. For example, as described earlier, the driver app includes a rating function that allows passengers to rate drivers and vice versa. To do so, the passenger in question needs the personal data of his Uber driver so that he can rate the quality of the ride and other aspects of the ride provided by the Uber driver. An average rating below the threshold could (previously) lead to exclusion from the platform, especially among drivers. Uber therefore exercises control over the quality of the services provided by their drivers. Uber cannot perform these activities without processing personal data. In particular, granting and denying access to the platform requires personal data about the Uber driver in question.
- As mentioned earlier, Uber assigns different classifications to Uber drivers such as Gold, Platinum or Diamond. In order to carry out these activities for the aforementioned purposes, Uber keeps information about drivers.
- Drivers who get a lot of rides are financially rewarded by Uber. Uber informs drivers where and when they can count on a large number of rides and/or preferred ride prices. Disagreements reported on the platform between a passenger and driver, for example about the fare, are also handled by Uber. Uber can unilaterally decide to refund the fare (in whole or in part) to the passenger, after which the driver is paid a lower amount for the ride.⁶⁹

94. Based on the above, it can be concluded that Uber's business in EEA territory and beyond consists of offering rides in a vehicle that is located and booked through its platform. The provision of this service forms the core of Uber's revenue model. The service is also offered and understood that way by applicants for rides. When ride applicants decide to use the Uber platform, they are looking for a transportation service that offers certain features and a specific standard of quality. Such aspects are predetermined and guaranteed by Uber. Therefore, the AP believes that Uber exercises control over important aspects of the transportation service offered through their platform. This type of control includes the collection and further processing of Uber drivers' personal data in the EEA, including the transfer of their personal data to third countries.

⁶⁸ C-434/15, *Asociación Profesional Élite Taxi v Uber Systems Spain SL*, ECLI:EU:C:2017:981, para. 48.

⁶⁹ Court of Amsterdam, ECLI:NL:RBAMS:2021:5029, r.o. 1.16.



Date

July 22,

Our

reference

95. In the present case, the AP expressly notes that the processing in question cannot be classified as "internal processing."⁷⁰ Indeed, there are two data controllers involved, UBV based in the EU and UTI based in the United States. These entities jointly determine the purposes and means of processing personal data of Uber drivers as described in situations 1 and 2. Furthermore, the data subjects in question have no control over these purposes and means of processing the personal data in question. Therefore, for the processing of personal data as described in Situations 1 and 2, the Uber drivers cannot be considered controllers within the meaning of the GDPR.
96. Finally, the third criterion requires that *"the importer is located in a third country (whether or not that importer is covered by the GDPR for the particular processing activity under Article 3) or is an international organization."* In the present case, UTI is geographically located in the United States and imports Uber drivers' personal data from the EEA to a third country within the meaning of the GDPR.

4.4.3 Conclusion

97. The AP concludes that the data transfer provisions in Chapter V GDPR are complementary to Article 3 GDPR. Transfers of personal data between joint controllers covered by Article 3 are not excluded from the GDPR's provisions on international transfers. This prevents that the protection provided by EU law with respect to personal data can be undermined or circumvented.
98. Second, it follows sufficiently clearly from Article 44 GDPR (and recital 101 GDPR) that movement of personal data from the Union to an entity in a third country constitutes a transfer. The AP notes that this case constitutes a transfer within the meaning of Article 44 GDPR, as personal data is transferred from the EEA to the United States (a third country). The AP further notes that all criteria for transfer as set forth in the Guidelines are also met. The personal data processing operations described in Situations 1 and 2 thus qualify as transfers from the EEA to the United States.⁷¹
99. The transfer by UBV to UTI means that the exporter, UBV, must comply with the obligations under the GDPR, including Chapter V GDPR. Finally, UBV must ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined. More specifically, UBV must assess whether the transfer instrument it intends to use is effective in light of the law and legal practice in force in the third country.⁷²

⁷⁰ In other words, where data are not transmitted or otherwise made available to another controller or processor by means of retransmission, even if that processing takes place outside the EU, see EDPB Guidance 05/2021 on the interplay between the application of Article 3 and the provisions on international transfers under Chapter V of the GDPR, margin 17.

⁷¹ Except for the case where personal data is sent by Uber from the US to the EEA when responding to requests from data subjects about the exercise of their GDPR rights.

⁷² EDPB Guidance 05/2021 on the interaction between the application of Article 3 and the provisions on international transfers under Chapter V of the GDPR, p. 15, marginal 25-27.



Date

July 22,

Our

reference

4.5 Did Uber have a transfer tool?

4.5.1 Legal framework

100. Article 45(1) GDPR states: *"A transfer of personal data to a third country or an international organization may take place if the Commission has decided that the third country, a territory or one or more specified sectors in that third country, or the international organization in question guarantees an adequate level of protection. No specific authorisation shall be required for any such transfer."*
101. On July 10, 2023, the European Commission adopted the Adequacy Decision. This Adequacy Decision has *"the effect that transfers by controllers and processors in the Union to certified organizations in the United States can take place without further consent. This is without prejudice to the direct application of Regulation (EU) 2016/679 to such entities, insofar as the conditions relating to the territorial scope laid down in Article 3 of that Regulation are met."*⁷³
102. Article 46(1) GDPR states: *"In the absence of a decision pursuant to Article 45(3), the transfer of personal data to a third country or an international organization by a controller or processor may take place only if they provide appropriate safeguards and the data subjects have enforceable rights and effective legal remedies."*
103. Article 46(2) GDPR stipulates that *"the appropriate safeguards referred to in paragraph 1 may be provided by the following instruments, without requiring specific consent of a supervisory authority:*
- a) a legally binding and enforceable instrument between government agencies or bodies;*
 - b) binding business rules corresponding to Article 47;*
 - c) standard data protection provisions adopted by the Commission in accordance with the examination procedure referred to in Article 93(2);*
 - d) standard data protection provisions adopted by a supervisory authority and approved by the Commission in accordance with the examination procedure referred to in Article 93(2);*
 - e) a code of conduct approved in accordance with Article 40, together with binding and enforceable commitments by the controller or processor in the third country to apply appropriate safeguards, including for the rights of data subjects; or*
 - f) a certification mechanism approved in accordance with Article 42, together with binding and enforceable commitments by the controller or processor in the third country to apply appropriate safeguards, including for the rights of the data subjects."*

Article 46(3) GDPR provides that *"subject to the consent of the competent supervisory authority, the appropriate safeguards referred to in paragraph 1 may also be provided by, in particular:*

- a) contractual provisions between the controller or processor, the processor or the recipient of personal data in the third country or international organization; or [...]"*

⁷³ European Commission Decision of July 10, 2023 on "the adequate level of protection of personal data under the EU-US Data Privacy Framework" (C2023/ 4745 final), marginal 8, p. 3.



Date

July 22,

Our

reference

4.5.2 Review

104. Article 44 GDPR describes the general principle on transfers, noting that the provisions of Chapter V should be applied so that the level of protection guaranteed by GDPR is not undermined when personal data are transferred to a third country.⁷⁴ Moreover, Chapter V is designed to ensure that the standard of protection arising from EU law is not circumvented through transfers of personal data to a third country for the purpose of processing there.⁷⁵
105. In the absence of an adequacy decision within the meaning of Article 45 of the GDPR, between July 16, 2020 and July 10, 2023, the transfer of personal data to the United States was allowed only on condition that appropriate safeguards were provided and data subjects had enforceable rights and effective remedies. In this regard, the AP considers that these appropriate safeguards provided by the data controller must ensure that the rights of the individuals whose data are transferred enjoy a level of protection that is essentially equivalent to that resulting from the GDPR, viewed in the light of the Charter.
106. The EDPB states in its guidelines that "*when an application is made to any of the transfer instruments mentioned in Article 46, GDPR, it should be assessed whether this ensures a level of data protection for the transferred data that is substantially equivalent to that guaranteed in the EU, or whether additional measures should be taken and when a controller or processor transfers data to an importer in a third country whose processing falls under Article 3(2) GDPR, the protection offered by the GDPR may also be undermined by the legal framework applicable to the importer.*"⁷⁶ The AP notes that where the GDPR is directly applicable based on Article 3(1) GDPR, the same reasoning can be followed when one of the joint controllers is located outside the Union. The AP further notes that when personal data are processed on EEA territory, they are protected not only by the provisions in the GDPR, but also by other EU and Member State laws. When personal data are transferred and/or accessed by entities outside the EEA territory, the overarching legal framework provided within the Union no longer applies. In this regard, Chapter V GDPR sets up a mechanism to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined. The data transfer mechanisms provide additional provisions to ensure the necessary safeguards to ensure that the protection afforded by the GDPR and the broader EEA legal framework is not undermined by foreign legislation, including when the GDPR is directly applicable on the basis of Article 3 GDPR.

⁷⁴ Recital 6 of the GDPR states that a "high level" of protection of personal data should be ensured both within the Union and in case of a transfer outside the Union. See also recital 101 of the GDPR.

⁷⁵ C-362/14, *Schrems*, ECLI:EU:C:2015:650, para. 73 and Conclusion 1/15, *EU Canada PNR Agreement*, ECLI:EU:C:2017:592, para. 214.

⁷⁶ EDPB Guidelines 5/2021 on the interplay between the application of Article 3 and the provisions on international transfers under Chapter V of the GDPR, p. 6, marginals 3 and 4. See further also EDPB Recommendations 01/2020 on measures complementary to onward transfer instruments to ensure compliance with the level of protection of personal data in the Union, EDPB Recommendations 02/2020 on European essential guarantees for surveillance measures and C-311/18, *Schrems II*, ECLI:EU:C:2020:559.



Date

July 22,

Our

reference

107. The EDPB's Guidelines further state that *"this means that the exporter must comply with the conditions of Chapter V when transferring the data using one of the instruments that are designed to protect the personal data after it has been transferred to a third country or an international organization."*
108. The AP found that from Aug. 6, 2021 to Nov. 27, 2023, UBV did not have a lawful transfer mechanism for the transfer of personal data from the EEA to the United States. In response to the AP's questions, Uber explains that *"UBV and UTI previously entered into the controller-to-controller standard contractual clauses of the European Commission ('SCCs') in their joint controllership agreement."* Uber adds that *"from the updated standard contractual clauses ('SCC') by the European Commission ('EC'), it follows that standard contract clauses do not apply to a controller whose processing is subject to the GDPR. In light of this Uber revisited its joint controller agreement to delete the SCCs."*⁷⁷ Uber thus removed from its Data Sharing Agreement the standard contract clauses for the transfer of personal data to third countries as of August 6, 2021 for this reason.
109. The European Commission (EC) stated in its FAQ that the relevant new standard contract clauses (SCCs) cannot be used in a situation where processing by controllers is directly subject to the GDPR.⁷⁸ Immediately after this, the EC notes that the *"European Commission is in the process of developing an additional set of SCCs for this scenario, which will take into account the requirements that already apply directly to those controllers and processors under the GDPR."* The AP believes that Uber could in no way have inferred from these statements that SCCs or other transfer instruments need not be used if the processing (by Uber's admission) falls under Article 3 GDPR. The EC's statement thus does not exempt Uber from compliance with the GDPR. Uber was and is currently required to use a pass-through instrument in accordance with Chapter V GDPR.⁷⁹
110. Uber should also have known, given its latest privacy statement, that a pass-through mechanism was required. In it, Uber stated that it adheres to the EU-US DPF and further states that: *"In the event that the EU-U.S. DPF or the Swiss-U.S. DPF are invalidated, Uber will transfer data that is subject to these certifications in reliance on the other data transfer mechanisms described above."*

4.5.3 Conclusion

111. The AP concludes that from August 6, 2021 to November 27, 2023, UBV (as exporter) did not have a lawful transfer mechanism for the transfer of personal data of drivers from the EEA to the United States. The AP did not receive an application from Uber regarding any other appropriate transfer mechanism.

⁷⁷ File No. 17, Uber's Response to Intelligence Request, dated Aug. 9, 2021, p. 6.

⁷⁸ EC, THE NEW STANDARD CONTRACTUAL CLAUSES - QUESTIONS AND ANSWERS, question 24, p. 13, available at: https://commission.europa.eu/system/files/2022-05/questions_answers_on_sccs_en.pdf

⁷⁹ The AP notes that depending on the situation in a particular third country, Article 46(2)(c) GDPR may require the controller to take additional measures to ensure the level of data protection within the Union, see C-311/18, *Schrems II*, ECLI:EU:C:2020:559, para. 133.



Date

July 22,

Our

reference

instruments under Article 46 GDPR received.⁸⁰ The AP therefore finds that Uber was in violation of Article 44 GDPR during the aforementioned period.

4.6 Can Uber successfully invoke a Section 49 GDPR exception?

4.6.1 Legal framework

112. Article 7 of the Charter states *"Everyone has the right to respect for his private and family life, his home and his communications."* Article 8(1) of the Charter states *"Everyone has the right to the protection of personal data concerning him or her."* Processing personal data, as defined in Article 4(2) GDPR, of a data subject affects the fundamental right to respect for private life guaranteed in Article 7 of the Charter. Moreover, such processing falls within the scope of Article 8 of the Charter.⁸¹ The AP notes that the rights enshrined in Articles 7 and 8 of the Charter are not absolute rights and must be considered in relation to their function in society.⁸² In addition to the above, Article 8(2) of the Charter states that personal data *"shall be processed fairly, for specified purposes and with the consent of the data subject or on any other legitimate basis for which the law provides."*
113. As regards the scope and interpretation of the rights and principles set out in the Charter, Article 52(1) of the Charter states that *"limitations on the exercise of the rights and freedoms recognised by this Charter shall be prescribed by law and shall respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."*⁸³
114. The derogations for specific situations set out in Article 49 GDPR state that *"in the absence of an adequacy decision according to Article 45(3) or appropriate safeguards according to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organization may take place only if one of the following conditions is met: [...]*
- b) *transmission is necessary for the performance of an agreement between the data subject and the controller or for the performance of pre-contractual measures taken at the request of the data subject;*

⁸⁰ Uber had voluntarily included and implemented the SCCs in their DSA. These were removed by Uber on its own initiative after the EC's new SCCs became available.

⁸¹ See, for example, C-92/09 and C-93/09, *Markus Schecke and Eifert*, EU:C:2010:662, at paras 49 and 52; C-594/12, *Digital Rights Ireland*, EU:C:2014:238, at para. 29

and Conclusion 1/15, *EU Canada PNR Agreement*, ECLI:EU:C:2017:592, marginals 122-123.

⁸² See, for example, C-92/09 and C-93/09, *Markus Schecke and Eifert*, EU:C:2010:662, at para. 48; C-291/12, *Schwartz*, EU:C: 2013:670, at para. 33; and Conclusion 1/15, *EU Canada PNR Agreement*, ECLI:EU:C:2017:592, at para. 136.

⁸³ Restrictions on the exercise of rights enshrined in the Charter must be made by law. This implies that the legal basis authorizing the interference must itself determine the scope of the restriction on the exercise of the right in question, see in this regard Conclusion 1/15, *EU Canada PNR Agreement*, ECLI:EU:C:2017:592, margin 139.



Date

July 22,

Our

reference

- c) *the transfer is necessary for the conclusion or performance of an agreement entered into in the interest of the data subject between the controller and another natural or legal person; [...]*
Where transfers not based on a provision of Articles 45 or 46, including those relating to binding corporate rules, are not covered by any of the exemptions for a specific situation referred to in the first subparagraph of this paragraph, the transfer to a third country or international organization may take place only if the transfer is non-repetitive, concerns a limited number of data subjects, is necessary for overriding legitimate interests of the controller and is not subordinate to the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the transfer and has provided appropriate safeguards for the protection of personal data on the basis of that assessment. The controller shall inform the supervisory authority about the transfer. In addition to the information referred to in Articles 13 and 14, the controller shall also inform the data subject about the transfer and the legitimate interests pursued. [...]"

115. Recital 111 of the GDPR states, "*Transfer should be possible in certain cases where the data subject has given his or her express consent, when the transfer is incidental and necessary in relation to a contract or a legal claim, regardless of whether the action is of a judicial, administrative or extrajudicial nature, including proceedings before regulatory bodies. [...]"*
116. The EPDB Guideline 2/2018 on Derogations under Article 49 of Regulation 2016/679, adopted on May 25, 2018, states, "*The EDPB notes that recital 111 uses the term 'incidental' and that the second paragraph of Article 49(1) uses the term 'non-repetitive' in the derogation based on 'compelling legitimate interests'. These terms indicate that similar transfers can happen more than once-not regularly-and should be part of the general approach, but for example, under random, unknown circumstances and at irregular intervals. Thus, a data transfer that takes place regularly within a stable relationship between the data export and a certain data import can generally be considered systematic and repetitive and therefore not incidental and not repetitive. [...]"*

4.6.2 Review

117. The AP notes that the processing operations (including transfers) that take place as described in Situations 1 and 2 with respect to personal data concerning Uber drivers fall within the scope of Articles 7 and 8 of the Charter. These provisions safeguard the fundamental rights of drivers. However, the AP notes that since these are not absolute rights, derogations limiting these rights are permissible only if they are consistent with Article 52 of the Charter. According to Article 52 of the Charter, derogations from these rights are only permissible if



Date

July 22,

Our

reference

these are established by law,⁸⁴ respect the essential content of those rights and freedoms,⁸⁵ and observe the principle of proportionality.⁸⁶

118. Article 49 GDPR provides that in the absence of an adequacy decision or appropriate safeguards, a transfer or a series of transfers of personal data to a third country can only take place provided the conditions of Article 49 GDPR are met. The AP notes that the derogations in this article should be interpreted restrictively and should only be used if strictly necessary.⁸⁷ After all, the derogations are intended for situations where there is no adequate protection in the country to which the data will be transferred, and where "*the risks for the data subjects are relatively small*" or because "*other interests*" outweigh them. For example, public interests or the interests of the data subject, which may outweigh the (other) data subject's right to privacy.⁸⁸ This principle is underscored in several provisions of Article 49 GDPR that place restrictions on its use⁸⁹ and the principle of derogations from fundamental rights under EU law.⁹⁰ The restrictive use of this article is also supported by the wording of to

⁸⁴ Restrictions on the exercise of a right enshrined in the Charter must be made by law. Where primary and secondary EU law is involved, it should be interpreted broadly. Further, the law must be in force and lawful. The legality requirement follows from Article 277 TFEU. Moreover, the law must be easily accessible and sufficiently precise, see ECHR, *Sunday Times v UK* (No. 1), CE: ECHR:1979:0426JUD000653874, para. 49. In assessing accessibility and sufficient precision, the foreseeability element is important, see with respect to this ECHR, *Open Door and Dublin Well Woman v Ireland*, CE: ECHR:1992:1029JUD001423488, r.o. 56-60.

⁸⁵ The essence of a right as described in Article 51(1) of the Charter is defined as its absolute inalienable core, see in this regard, for example, Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, *Kadi*, EU:C:2013:518, para. 134. According to the Opinion of A-G Saugmandscaard Øe, the requirement set out in Article 52(1) of the Charter that any restriction on the exercise of the rights and freedoms recognized in that instrument must respect the essence of those rights and freedoms means that a measure infringing that essence cannot be justified. That measure is then deemed to be contrary to the Charter and must be annulled or invalidated as a *U n i o n* act, without it being necessary to examine the condition of compliance with the principle of proportionality, see, to this effect, the Conclusion of the A-G in C-401/19, *Republic of Poland v European Parliament*, ECLI:EU:C:2021:613, marginal 98-99. Furthermore, "[...] The

"substantial content" of a fundamental right constitutes an "inviolable core" that must remain free from interference. Accordingly, certain, exceptionally serious assaults on fundamental rights are not justified by any end, however legitimate. In other words, the end does not justify all means." See also Conclusion A-G in C311/18, *Schrems II*, ECLI:EU:C:2020:559, para. 272. This view is reiterated in the Conclusion of Advocate General Guivanni Pitruzzella in C-817/19, *Human Rights League v Council of Ministers*, EU:C:2022:65. More specifically, it states, "Moreover, it is clear both from the wording of Article 52(1) of the Charter and from the case law of the Court, and in particular from the *Schrems I* judgment, that the assessment of whether the essential content of the fundamental right in question has been affected must be made prior to and independently of the proportionality assessment of the challenged measure. In other words, it is an independent test." Ministers delivered January 27, 2022 (the Conclusion is translated from French as no English version is available).

⁸⁶ See Article 52(1) of the Charter and the case law of the CJEU, see e.g. C5/88, *Wachauf*, EU:C:1989:321, para. 18. The principle of proportionality is a general principle in European law to which a four-part test is applied: 1) does the measure pursue a legitimate aim, 2) is the measure appropriate to achieve that aim, 3) is it the least restrictive available measure by which the aim can be achieved as well as by the chosen measure, and 4) are the conflicting interests appropriately balanced.

⁸⁷ The CJEU underlined that the protection of the fundamental right to respect for private life at EU level requires that derogations and limitations to the protection of personal data apply only to the extent strictly necessary, see C 73/07, *Satakunnan Markkinapörssi and Satamedia*, ECLI:EU:C:2008:727, r.o. 56; C 92/09 and C 93/09, *Volker und Markus Schecke and Eifert*, ECLI:EU:C:2010:662, para. 77; C-293/12 and C-594/12, *Digital Rights Ireland*, EU:C:2014:238, para. 52, C 362/14, *Schrems*, ECLI:EU:C:2015:650, para. 92, C 203/15, *Tele2 Sverige AB*, ECLI:EU:C:2016:970, para. 96.

⁸⁸ See, for example, C-362/14, *Schrems*, ECLI:EU:C:2015:650, at para. 92 and C-293/12 and C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, at para. 52.

⁸⁹ Article 49(2-4) GDPR.

⁹⁰ C-362/14, *Schrems*, ECLI:EU:C:2015:650, para. 92 and C-293/12 and C-594/12, *Digital Rights Ireland*, ECLI:EU:C:2014:238, para. 52.



Date

July 22,

Our

reference

Article 49 GDPR given title stating that the derogations may only be used for specific situations.⁹¹

119. Furthermore, the AP notes that the use of Article 49 GDPR does not provide additional protection or safeguards for transfers of personal data that may lead to an increased risk with respect to the rights and freedoms of the data subjects concerned. Moreover, the AP notes that when the transfer is based on a derogation, the relevant provisions of the GDPR still apply.⁹² Finally, Article 49 GDPR should be read in light of the Charter.⁹³
120. Uber indicated that if the AP concludes that there are processing operations that qualify as transfers within the meaning of Chapter V GDPR, Uber could base the processing operations described for situation 1 on Article 49(1)(b) GDPR.⁹⁴ The processing operations described for situation 2 could, according to Uber, be based on Article 49(1)(c) GDPR.⁹⁵ Below, the AP assesses Uber's reliance on these two grounds for exception in the respective order.

The pass-throughs are not incidental

121. Based on recital 111 to the GDPR, this derogation may only be used if the transfer is incidental. As indicated in the EDPB Guidelines, this excludes transfers that "*occur regularly within a stable relationship*" and cannot apply "*to frequent transfers within the business relationship*."⁹⁶ Any other interpretation would not be consistent with EU law, which requires that a derogation from a fundamental right not be interpreted in a way that contradicts its exceptional nature.⁹⁷
122. The AP notes that to justify transfer activities as described for situation 1, the derogation on contractual necessity of Article 49(1)(b) GDPR cannot be invoked. This is because the transfers of data of more than [confidential] Uber drivers between UBV and UTI are considered systematic, repetitive and ongoing. In that respect, in line with the EDPB Guidelines, the AP notes that in light of recital 111, one only relies on Article 49(1)(b), (c) and (e)

⁹¹ EDPB Guidelines 2/2018 on derogations under Article 49 of Regulation 2016/679, adopted May 25, 2018, p. 4.

⁹² Article 44 GDPR states that transfers of personal data under Chapter V are only "*without prejudice to the other provisions of this Regulation*." can take place.

⁹³ C-617/10, *Akerberg Fransson*, ECLI:EU:C:2013:280, para. 21.

⁹⁴ See "*Views of Uber on Investigation Report and Intent to Enforce*," June 9, 2023, r. 236, pp. 58-59 and pp. 71-73 (Section 7.3.4.).

⁹⁵ See "*Views of Uber on Investigation Report and Intent to Enforce*," June 9, 2023, r. 236, pp. 58-59 and pp. 67-71 (Section 7.3.3).

⁹⁶ EDPB Guidance 2/2018 on derogations under Article 49 of Regulation 2016/679, p. 11: *Data transfers that occur regularly in a stable relationship are considered systematic and repetitive and are therefore no longer "incidental" in nature. Consequently, many data transfers within a business relationship cannot be based on Article 49(1)(b) in this case.*

⁹⁷ C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, ECLI:EU:C:2020:790, para. 69. Furthermore, when a provision "*provides for an exception to the general rule, it must, according to settled case law, be interpreted strictly. That provision must therefore not allow the exception to the mandatory principle ... become the rule, because in that case the latter provision would largely lose its substance.*" , see C-140/20, *Dwyer v Commission for An Garda Síochána*, ECLI:EU:C:2022:258, para. 40. See, e.g., C-203/15 and C-698/15, *Tele2 Sverige AB*, EU:C:2016:970, para. 89, C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, EU:C:2020:791, para. 111.

AUTORITEIT
PERSOONSGEGEVENS

Date

July 22,

Our

reference

GDPR may be invoked to justify incidental transfers.⁹⁸ This view is supported by the general view within Union law, where it is established practice to interpret derogations restrictively, and that any limitations or derogations from Articles 7 and 8 of the Charter are permissible only to the extent deemed strictly necessary.⁹⁹ The CJEU has taken this position on many occasions, stating that a situation where the exception becomes the rule should be avoided.¹⁰⁰

123. Uber has stated that the AP's explanation is incorrect and incompatible with Article 49 GDPR. Uber substantiates its claims by invoking the non-binding nature of the GDPR's recitals. Uber argues that the criterion "incidental" is not set forth in Article 49 GDPR. The wording of Article 49(1) GDPR, which provides that the derogations may be used in specific situations for a "transfer" or "series of transfers," does not imply, according to Uber, that the provision can be interpreted to mean that "incidental" is part of the criteria that must be met.
124. The AP agrees with Uber that the recital has no binding legal force and cannot be invoked as a basis to deviate from actual provisions of the law or in the case where provisions are interpreted in such a way that clearly contradicts the wording of the provision. However, the AP notes that the recitals to the GDPR *"can explain the content of the provisions of that law"* and that it *"contains important elements of interpretation, which clarify the intentions of those who drafted the law."*¹⁰¹ More importantly, the CJEU supports this interpretation in its jurisprudence, where it explained limits to the scope of the derogation in light of the recitals. More specifically, the ECJ considers that the interpretation of a provision of EU law requires not only the wording but also *"the context in which it takes place and the objective pursued by the rules of which it forms part"*¹⁰² and that *"the scope of the derogation...must be determined in the light of the interpretation thus given by the EU legislature."*¹⁰³ The ECJ further held that to interpret the derogation without regard to the intention of the EU legislator expressed in the recitals would be detrimental to the purpose of the legislation.¹⁰⁴ Therefore, the AP finds that Recital 111 to the GDPR provides the necessary clarification in interpreting Article 49(1)(b) GDPR in line with the objectives pursued by the EU legislator and also finds that the recital does not contradict the wording of the aforementioned article. A different interpretation of this article would ignore the intention of the legislator and be contrary to the approach adopted by the CJEU.¹⁰⁵ The AP therefore comes to the

⁹⁸ EDPB Guidelines 2/2018 on derogations under Article 49 of Regulation 2016/679.

⁹⁹ C-623/17, *Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others*, ECLI:EU:C:2020:790, para. 81; C-203/15 and C-698/15, *Tele2 Sverige AB*, EU:C:2016:970; C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, EU:C:2020:791, r.o. 130; C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd*, ECLI:EU:C:2020:559, r.o. 176; Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications*, ECLI:EU:C:2014:238, para. 52; C-362/14, *Schrems*, ECLI:EU:C:2015:650, para. 96.

¹⁰⁰ See, e.g., C-140/20, *Dwyer v Commission for An Garda Síochána*, ECLI:EU:C:2022:258, para. 40; C-817/19, *Ligue des droits humains*, ECLI:EU:C:2022:491, at 114; C-401/19, *Republic of Poland v European Parliament and the Council of the European Union*, EU:C:2022:297, at 64 and 74.

¹⁰¹ C-418/18, *Puppinck and others v Commission of the European Communities*, ECLI:EU:C:2019:1113, para. 75.

¹⁰² C-528/16, *Confédération paysanne and Others*, EU:C:2018:583, para. 42.

¹⁰³ *Ibid.*, r.o. 44-46.

¹⁰⁴ *Ibid.*, r.o. 51-53.

¹⁰⁵ *Ibid.*, see also, e.g., C424/10 and C425/10, *Ziolkowski v Land Berlin*, ECLI:EU:C:2011:866, para. 42-43.



Date

July 22,

Our

reference

conclusion that only Article 49(1)(b) GDPR can be invoked to justify "incidental" transfers.

125. With respect to the processing described for situation 1, UBV cannot rely on the derogation of Article 49(1)(b) GDPR in the present case to justify the transfer to the United States. Indeed, that transfer qualifies the AP as systematic, repetitive and ongoing in a stable, ongoing business relationship between UBV and UTI.
126. As for the processing operations in situation 2, Uber indicates that they can be based on Article 49(1)(c) GDPR. Under this derogation, transfers or a series of transfers may take place when "*the transfers are necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person.*" The condition that the transfer must be necessary and incidental also applies to this provision. In the present case, UBV cannot use the derogation as a basis for transfer, because this transfer is also considered systematic and repetitive in nature within a stable, ongoing business relationship between UBV and UTI. Moreover, Uber has a legal duty to facilitate data subjects' rights not under the agreement, but under GDPR.
- The transfers are not necessary
127. Besides the fact that there is no incidental transfer, Uber also cannot successfully invoke Article 49 (1) (b) and (c) GDPR because the transfer is not necessary for the implementation of an agreement between Uber and the data subject or between Uber and a third party (an agreement in the interest of the data subject), respectively.
128. In this regard, the AP recalls that the necessity requirement, as an autonomous Union concept, requires that the processing must be *objectively indispensable* for the accomplishment of the contract.¹⁰⁶ It is irrelevant here whether the processing is useful for the contract or mentioned therein,¹⁰⁷ on the contrary, the controller must demonstrate that the main purpose of the contract could not be achieved without such processing.¹⁰⁸ The necessity link must, as Uber itself rightly points out, be close and substantial in relation to the purpose of the agreement.
129. An example of necessity is when a data transfer takes place from a travel agency to a hotel in a third country in order to establish a contract between the customer and the travel agency. In this case, the connection between the transfer and the purpose is close and substantial, and no realistic alternative is available (hotels are now often located in third countries). An example of a lack of necessity is when a business group for business purposes transfers its

¹⁰⁶ CJEU judgment of July 4, 2023 *Meta* (ECLI:EU:C:2023:537), ro. 98.

¹⁰⁷ CJEU Judgment of July 4, 2023 *Meta* (ECLI:EU:C:2023:537), para. 99 and A-G's Opinion, para. 54.

¹⁰⁸ CJEU judgment of July 4, 2023 *Meta* (ECLI:EU:C:2023:537), ro. 98.



Date

July 22,

Our

reference

centralized payment functions and personnel management for all its personnel in a third country, as there is no objective link between the execution of agreement and the transfer.¹⁰⁹

130. Uber explained the necessity in the present case by first pointing out that the transfer takes place in the context of the agreements (*Data Sharing Agreement*) between UBV in the EU and UTI in the US. In the AP's view, this does not make the transfer necessary, precisely because the Court has held that the mere existence of the agreement itself (the "mentioning") cannot constitute necessity. To assume necessity, the Court said, there must be "no practicable, less intrusive alternatives" and the data controller must be able to demonstrate this.¹¹⁰
131. Secondly, Uber believes that centralized data processing in the U.S. is crucial to being able to offer Uber services and to ensuring drivers' rights in the EU to protection of their personal data: 'only by processing personal data centrally can Uber apply its comprehensive technical and organizational measures worldwide and provide drivers with the highest level of protection.' Uber has not been able to make it sufficiently clear to the AP why the transfer of personal data to the U.S. is crucial for providing the service and a high level of protection. First, as mentioned in margin number 128, there is a lack of necessity when a business group centralizes personal data in a third country for business purposes. In this case, the personal data could also have been processed on a server in the EU if a third country does not provide an adequate level of protection. Second, it seems, in almost every conceivable case, that a transfer to a country without an adequate level of protection actually compromises the level of protection provided by the GDPR.
132. Perhaps needless to say, although Uber stated in its written submission that the transfer is crucial for both offering the services and providing a higher level of data protection, Uber's explanations at the submission hearing suggest that other motives may have been at play. Uber stated that the choice of centralized processing in the U.S. was motivated by the fact that the service could be delivered faster and more efficiently that way.¹¹¹ With that, the centralized processing seems to have been motivated precisely by reasons much more akin to its efficiency in the US.¹¹²
133. In summary, the AP considers that Uber has not demonstrated why the transfer is objectively necessary for the performance of the agreement and that no useful, less intrusive alternatives are available. Reliance on Article 49(1)(b) and (c) GDPR therefore also fails for this reason.

¹⁰⁹ EDPB Guidelines 2/2018 on derogations under Article 49 of Regulation 2016/679, p. 10.

¹¹⁰ CJEU judgment of July 4, 2023 *Meta* (ECLI:EU:C:2023:537), para. 99.

¹¹¹ See the minutes of the view session held on July 5, 2023, p. 6.

¹¹² Cf. CJEU Judgment of July 4, 2023 *Meta* (ECLI:EU:C:2023:537), para. 99: on the contrary, the Court explicitly states that being "useful" does not constitute a necessity.



Date

July 22,

Our

reference

4.6.3 Conclusion

134. The AP concludes that for the period from August 6, 2021 to November 27, 2023, Uber cannot successfully invoke the derogations (exceptions) for specific situations in relation to international transfers referred to in Article 49(1)(b) and (c) GDPR.

4.7 Final conclusion

135. The AP considers that there is processing involving personal data of Uber drivers from the EEA by Uber. In addition, there is a transfer of personal data within the meaning of the GDPR. In the absence of an adequacy decision, within the meaning of Article 45 of the GDPR, between July 16, 2020 and July 10, 2023, the transfer of personal data to the United States was allowed to take place only subject to appropriate safeguards and subject to enforceable rights and effective legal remedies. The AP found that, at least between August 6, 2021 and November 27, 2023, UBV did not provide the necessary appropriate safeguards described in Article 46(2) GDPR. Furthermore, UBV (given the non-emergency and structural nature of the processing operations) cannot successfully invoke the exceptions described in Article 49(1)(b) and (c) GDPR. The AP therefore finds that Uber was in breach of Article 44 GDPR during the aforementioned period.

5. The fine

5.1 Penalty power and view of Uber

136. Uber raised several grounds related to the lack of justification for the AP's imposition of an administrative fine or remedy. First, Uber argues that the investigation report was flawed and carelessly drafted. Second, according to Uber, the lex-certa principle and the fact that there is a prospect of concrete legalization (by the EU-US DPF) opposes enforcement by the AP. Third, according to Uber, citing ECJ case C-807/21, an administrative fine can only be imposed if there is intent or negligence and a remedial measure is not appropriate. Lastly, Uber argues that a measure may have disproportionate consequences and that Uber should therefore be allowed, upon having more definite information about the possible sanction decision, to submit a separate view on it.
137. The AP does not follow Uber's argument. The AP is of the opinion that based on the facts and the assessments based thereon, it has been established beyond reasonable doubt that a transfer of personal data takes place and that the violation was committed by Uber. Where necessary, the AP has supplemented the facts and assessments in response to Uber's views. With regard to Uber's reliance on the lex certa principle, which is enshrined in Article 49 of the Charter, among other things, the AP considers the following. As the Administrative Law Division of the Council of State has repeatedly held,¹¹³

See, among others, rulings of July 9, 2014, ECLI:NL:RVS:2014:2493, January 16, 2019, ECLI:NL:RVS:2019:109.



Date

July 22,

Our

reference

the *lex certa* principle requires the legislator, for the sake of legal certainty, to define prohibited conduct in as clear a manner as possible. It should be borne in mind that the legislator sometimes defines prohibited conduct with a certain vagueness, consisting of the use of general terms, in order to prevent conduct worthy of punishment from falling outside the scope of that definition. This vagueness may be unavoidable, because it is not always foreseeable in what way the interests to be protected will be violated in the future and because, if this can be foreseen, the descriptions of prohibited conduct would otherwise become too refined, with the result that the clarity is lost and thus the interest of the general clarity of legislation suffers. In other words, the *lex certa* principle requires the legislator, for the sake of legal certainty, to define prohibited conduct in as clear a manner as possible.¹¹⁴

138. The AP concludes that this is the case. According to the AP, the provisions it has reviewed are sufficiently clear. Based on Chapter V GDPR, the recitals to the GDPR, the case law on transfers by the CJEU and also previous decisions by other European privacy regulators, it was foreseeable for Uber that a transfer instrument would be necessary for the transfer of personal data to the United States (as a third country). The fact that Uber became certified under the new adequacy decision on November 27, 2023, does not diminish the AP's authority to take enforcement action for the period of two years and three months during which Uber did not have a transfer instrument. Therefore, based on the facts and the assessments based thereon, it is established beyond reasonable doubt that the violation was committed by Uber.
139. The AP has the power to impose an administrative fine under Article 58(2) opening words and under i, in conjunction with Article 83 of the GDPR and read in conjunction with Article 14(3) of the GDPR Implementation Act. In this context, the CJEU first specified that a prerequisite for the imposition of such a fine is that the breach was culpably committed by the infringer. This includes intentional or negligent conduct. A controller has committed an infringement intentionally or negligently if he could not have been unaware that his conduct constituted an infringement, regardless of whether he was aware that he was violating the provisions of the GDPR, it follows from the case law of the CJEU.¹¹⁵
140. The AP found that Uber committed a violation of Article 44 GDPR. Uber could have known on the basis of the GDPR and the case law of the CJEU that the transfer of personal data to the United States requires a transfer instrument. Because of this violation and its seriousness, the AP sees reason to use its power to impose an administrative fine.
141. Finally, with regard to Uber's position that it was wrongly not given the opportunity to submit an opinion on the level of the fine, the severity and extent of the violation found and the final substantiation, the AP considers the following. Neither Section 4:8 nor Section 5:50 of the Awb (read in conjunction with Sections 5:48 and 5:53 of the Awb) obliges the AP to

¹¹⁴ Ruling of October 26, 2022, ECLI:NL:RVS:2022:3077. See also ECHR, November 11, 1996, no.17862/91, ECLI:CE:ECHR:1996:1115JUD001786291.

¹¹⁵ ECJ-EU, Case C-807/21, December 5, 2023, ECLI:EU:C:2023:950, paragraphs 75 and 76.



Date

July 22,

Our

reference

to comment on these aspects as early as the intention to impose an administrative fine.¹¹⁶ An intention to impose a fine and the investigation report based on it are sufficient on the basis of which an opinion can be requested. The AP here reminds Uber of the objection phase, where Uber can still object (and must be heard) to the amount of the fine and its substantiation. Incidentally, the AP has included the submitted opinion in its assessment.

What is mentioned in the view may contribute to the AP's decision to proceed with the imposition of an administrative fine, after which the AP determines the level of the fine based on all relevant facts and circumstances known to it at the time. For this reason, the AP did not comment on the aspects mentioned by Uber in its intention to enforce.

5.2 Systematic determination of penalty level

142. The EDPB agreed to the final text of the Guidelines 04/2022 on the calculation of administrative fines under the GDPR (hereinafter, the Guidelines) at its plenary meeting on May 24, 2023. The AP will apply these Guidelines to this case.¹¹⁷ The AP's (national) policy rules on determining the amount of administrative fines have been repealed, insofar as currently relevant.¹¹⁸

143. The Guidelines describe a methodology that considers successively:

1. Identify the processing activities in the case in question and evaluate the application of Article 83(3) GDPR;
2. Determine the starting amount for further calculation;
3. Whether there are extenuating or aggravating circumstances that require adjustment of the amount from Step 2;
4. What maximum amounts apply to the violations and whether any increases from the previous step do not exceed this amount;
5. Whether the final amount of the fine calculated meets the requirements of effectiveness, deterrence and proportionality, and is adjusted accordingly if necessary.

144. These steps are completed in sequence below.

5.3 Penalty amount calculation

5.3.1 Step 1: Identify acts and violations

145. To determine the starting amount of the fine, as described in the Guidelines, the first thing to consider is whether there is one or more sanctionable conduct.

¹¹⁶ CBB May 7, 2019, ECLI:NL:CBB:2019:177

¹¹⁷ See also <https://www.autoriteitpersoonsgegevens.nl/actueel/nieuw-boetebeleid-voor-overtredingen-avg>

¹¹⁸ See <https://www.autoriteitpersoonsgegevens.nl/documenten/boetebeleidsregels-autoriteit-persoonsgegevens-2023>



Date

July 22,

Our

reference

146. The AP found that there was a lack of one of the transfer instruments laid down in Chapter V GDPR. By doing so, Uber has violated the obligation under Article 44 GDPR to use a transfer instrument in international transfers. The calculation of the starting amount in this case relates to two processing activities that fall within the context of one sanctionable conduct.

5.3.2 Step 2: Determine starting amount

147. As described in the Guidelines, the starting amount of the fine level should then be determined. This starting amount is the starting point for further calculation in later steps, taking into account all relevant facts and circumstances. The Guidelines state that the starting amount is determined on the basis of three elements: i) the classification of infringements according to Article 83 paragraphs 4 to 6 GDPR; ii) the gravity of the infringement and iii) the turnover of the undertaking. All three elements are discussed below.

Re i) Classification of breaches according to Article 83(4-6) of the GDPR

148. As mentioned in the Guidelines, almost all obligations of the data controller are categorized in the provisions of Art. 83 paragraphs 4 to 6 GDPR. The GDPR distinguishes between two types of breaches. On the one hand, the breaches that are sanctionable under Art. 83 paragraph 4 GDPR, and for which a maximum fine of €10 million (or in the case of a company, 2% of annual turnover, whichever is higher) applies, and on the other hand, the breaches that are sanctionable under Art. 83 paragraphs 5 and 6 GDPR, and for which a maximum fine of €20 million (or in the case of a company, 4% of annual turnover, whichever is higher) applies. With this distinction, the legislator provided an initial indication of the severity of the breach: the more serious the breach, the higher the fine.
149. For the currently present violation of Art. 44 GDPR, an administrative fine of up to €20,000,000.00 (or in the case of a company, 4% of its worldwide annual turnover, whichever is higher) may be imposed. It follows from this categorization that the violation of these provisions are considered serious (in the abstract) by the legislator.

Re ii) Gravity of the infringement

150. In determining the severity of the breach, the 1) nature, 2) severity and 3) duration of the breach, as well as the intentional or negligent nature of the breach and the categories of personal data involved should be taken into account.
151. The nature of the breach should consider the interest that the breached provision is intended to protect. The AP finds that the intended interest of Article 44 GDPR, namely the continuity of the GDPR's high level of protection when transferring personal data to third countries, was not ensured by Uber. In the absence of an adequacy decision or appropriate safeguards during the period of the breach, Uber unlawfully transferred personal data to a third



Date

July 22,

Our

reference

country when that third country has an inadequate level of protection. Specifically, this involves transfers to the United States, where intelligence agencies have access to personal data of EU citizens under local law. This breach directly threatens the right to private life and the right to the protection of personal data enshrined in Articles 7 and 8 of the Charter, respectively.

152. To assess the seriousness of the violation, the AP considers the following. Regarding the nature of the processing, it is first relevant to consider the relationship between the controller and the data subjects. The AP notes that in this case there is a hierarchical working relationship between Uber and the drivers.¹¹⁹ The AP notes, as described in Section 4.3.2, that Uber's actual *modus operandi* towards its drivers also assumes a high degree of dependency. Uber itself confirms this in its written view by stating in it that the drivers "depend for their daily livelihood on the income they obtain through the Uber Rides driver app."¹²⁰ Second, the nature of the processing involves higher risks because Uber evaluates personal aspects of drivers and makes decisions about them.
153. Regarding the scope of the processing, the AP notes that there is cross-border processing within the meaning of Article 4, section 23, GDPR. Uber processes personal data of drivers from several EU countries. This makes Uber's processing extensive.
154. Regarding the purpose of the processing, the AP notes that the more central the location of the processing within the core activities of the controller, the more serious will be irregularities in that processing.¹²¹ In this assessment, processing in the context of trip generation should be distinguished from handling inspection requests. As for the processing of personal data in the context of generating rides, the AP notes that this is an essential part of Uber's core business of mediating as a platform between drivers offering rides and customers requesting rides. Without generating rides, it is not possible to suggest rides to drivers, and for them to accept and offer them to customers. As for the processing of personal data for the purpose of handling inspection requests, the AP notes that this is not part of Uber's core business, as Uber is merely trying to comply with a legal obligation that follows from the GDPR. In doing so, it does not independently contribute to Uber's revenue model as a commercial enterprise.
155. Regarding the number of affected data subjects, the AP found that from August 6, 2021 through mid-February 2023, there were an average of [confidential] drivers active for Uber in France and an average of [confidential] drivers across the EU. As of Feb. 17, 2023, there were [confidential] active drivers in the EU according to Uber. Regarding transfers in the context of inspection requests, between August 2021 and February 2023, Uber conducted [confidential] inspection requests with the

¹¹⁹ See also French Court of Cassation, March 4, 2020 (Sentencia n°374); Rb. Amsterdam, Sept. 13, 2021 (ECLI:NL:RBAMS:2021:5029), rulings 27 to 32.

¹²⁰ 'Views of Uber on Investigation Report and Intent to Enforce' dated June 9, 2023, p. 83.

¹²¹ Guidelines 04/2022 for the calculation of administrative fines under the GDPR, marg. 54.



Date

July 22,

Our

reference

automatic download tool of drivers from the EU. Uber also conducted [confidential] removal requests for EU (former) drivers. Finally, Uber states that, in addition to the download tool, Uber processed [confidential] requests from French (former) drivers for expanded access requests between August 6, 2021 and February 1, 2023. In addition, Uber states in its written view that as part of its handling of inspection requests by phone and letter, fewer than 10 requests are handled per year. Some requests are too complex and have to be prepared manually by an employee of Uber B.V. In that context, it is about 100 requests in the first four months of 2023.

156. The AP further found in Section 2.5 that the breach occurred from Aug. 6, 2021 to Nov. 27, 2023. That is two years and more than three months. This represents a significant period of time. In the AP's view, Uber culpably committed the conduct. The breach ceased to exist as of Nov. 27, 2023, because Uber certified under the EU-US DPF on that date.
157. Finally, it should be considered whether Uber has processed personal data that deserves special protection and therefore leads to a higher severity of the breach. The amount of data collected on each data subject must also be taken into account. As the AP found in Section 2.3, Uber processes a large amount of data about Uber drivers. In addition to account data, location data, photos, payment receipts and ratings, Uber also processes (depending on the legal rules in a country) other data, such as ID, criminal and health data. Much of this data is sensitive by its nature. In addition, criminal and health data are special personal data that enjoy additional protection under Article 9 and Article 10 GDPR. In particular, the AP blames Uber for the transfer of criminal data to the United States, which, at the time, was determined not to be able to provide an adequate level of protection, and where it was known that government agencies could access personal data stored there. For the above reasons, the AP considers the impact of this aspect increasing the overall severity of the breach.

Re iii) Turnover of the company

158. The Guidelines require that for reasons of fairness, the starting amount of the fine should be related to the size of the undertaking. The size of the undertaking is determined on the basis of turnover. For example, for a small undertaking, with a turnover not exceeding €2 million, the starting amount is generally limited to 0.2 to 0.4% of the actual starting amount, and the starting amount increases as the undertaking's turnover increases. If a company's turnover exceeds €500 million, the fine level is set at a percentage of the company's annual turnover.¹²² As a result, the size and turnover of the company is already factored into the amount of the fine, so the starting amount does not need adjustment on that ground.

¹²² From an annual turnover of €500 million, 4% of the annual turnover exceeds €20 million, so that this percentage must be taken into account as the penalty ceiling (Article 83, fifth paragraph, introductory sentence of the GDPR).



Date

July 22,

Our

reference

159. As mentioned in recital 150 of the GDPR, when imposing a fine on an undertaking, the "undertaking" should be considered an undertaking under Articles 101 and 102 of the Treaty on the Functioning of the European Union. It follows from established case law of the CJEU that an undertaking is any entity engaged in an economic activity, regardless of its legal form and how it is financed. Thus, what matters is the economic unit of the enterprise and not the legal entities within it. Several companies or entities within the same economic unit may therefore together constitute an undertaking within the meaning of the aforementioned provisions.
160. Uber B.V. is indirectly a wholly owned subsidiary of Uber Technologies Inc. They should therefore be considered part of the same company for the purposes of Article 83 of the GDPR.
161. As stated in the Guidelines, turnover can be determined on the basis of the company's annual records for the previous fiscal year. Pursuant to Article 83(4-6) of the GDPR, the worldwide turnover for the previous fiscal year is taken into account.
162. Uber Technologies Inc. has published its annual financial statements for 2023 on its website.¹²³ A consolidated overview of the company is included on page 75. It shows that the company's global revenue for 2023 is \$37.281 billion. That corresponds to €34.235 billion.¹²⁴

Determining starting amount

163. Pursuant to Article 83(5) of the GDPR, the penalty ceiling is 4% of annual turnover. The annual turnover is €34.235 billion, so the penalty ceiling for the violation is €1.369 billion.
164. The appreciation of the above circumstances and factors determines the overall gravity of the infringement committed by Uber. This involves a thorough assessment of the concrete circumstances of the case in which all the circumstances must be considered in context.
165. In view of what has been considered in (i) and (ii) above, the AP takes the view that the level of gravity of the infringement should be qualified as "high." According to the Guidelines, for infringements with a high level of severity, the starting amount should be set at a point between 20% and 100% of the fine maximum of €1.369 billion in this case. This corresponds to an amount between the €273.881 million and €1.369 billion. The general rule here is that the more serious the infringement is within its own category, the higher the starting amount will be.

¹²³ Available at <https://investor.uber.com/financials/default.aspx>

¹²⁴ Total sales for 2023 were \$37,281,000,000, which with an exchange rate dated July 19, 2024 of \$1 at 0.9183 converts to sales of € 34.235.142.300.



Date

July 22,

Our

reference

166. The AP believes that, given the circumstances described, the violation is serious. However, the AP does not consider all circumstances so serious or adverse that the starting amount should be set at the upper limit of the penalty ceiling. Among other things, the AP considered the size of the number of affected data subjects and the circumstance that the breach has ended.

167. Based on the categorization of the breach, the severity of the breach and the company's turnover, the AP sets the starting amount for the violation of Article 44 GDPR in this case at €290 million.

5.3.3 Step 3: Assess other relevant circumstances

168. As stated in the Guidelines, it should then be considered whether the circumstances of the case warrant setting the fine higher or lower than the starting amount determined above. The circumstances to be taken into account are listed in Article 83, second paragraph, opening words and points (a) to (k) of the GDPR. The circumstances listed in that provision must each be considered only once. In the previous step, the nature, gravity and duration of the breach (part a), the intentional or negligent nature of the breach (part b) and the categories of personal data (part g) have already been considered. This leaves parts c through f and h through k.

169. The only applicable circumstance is how the AP became aware of the breach, in particular whether, and if so to what extent, the controller reported the breach (section h). In this case, Uber did not report the breaches itself, but came to the AP's attention through complaints. However, according to the Guidelines, this is assessed as "neutral" and therefore has no impact on the amount of the fine to be imposed.

5.3.4 Step 4: Verification exceeding maximum amounts applicable to the violations

170. As mentioned, - also considering Uber's turnover - the observed violation is subject to a maximum fine level of 4% of the company's annual worldwide turnover. The annual turnover amounts to €34.235 billion, so the penalty ceiling for the offense is €1.369 billion.

171. Based on the above considerations, the AP sets the fine amount for the violation found at €290 million. This is below the statutory maximum so that no excess occurs.

5.3.5 Step 5: Assessment requirements of effectiveness, proportionality and deterrence

172. Finally, it must be assessed whether the fine is effective, proportionate and dissuasive. In addition, given the circumstances of the case, the administrative fine should not lead to a disproportionate outcome.

173. The Guidelines prescribe that the imposition of an administrative fine can be considered effective if it achieves the purpose for which it was imposed. The purpose may be to punish unlawful conduct as well as to promote compliance with applicable regulations. Given the



AUTORITEIT
PERSOONSGEGEVENS

Date

July 22,

Our

reference

above considerations regarding the nature, gravity and duration of the breach, as well as the aggravating and mitigating circumstances of Article 83(2) GDPR, the AP considers that the present administrative fine achieves both goals and is therefore effective and dissuasive.

174. The AP further believes that the imposition of the fine and its amount, due to the severity of the violation and the size of the company, is not disproportionate. Uber indicated in its submission that the imposition of an administrative fine would lead to disproportionate consequences for Uber, as any notification about the fine to the New York Stock Exchange could have significant consequences on Uber's share price. However, the AP sees no reason in this to consider the fine disproportionate. While it cannot be ruled out that the fine may have some impact on Uber's share price, it has not been made plausible that this is of such an impact that the fine should be deemed disproportionate. It is also important here that the amount of the fine must be sufficiently dissuasive and do justice to the nature and gravity of the violation. In the AP's view, no other special circumstances have arisen in this regard that would make the fine disproportionate.
175. For the sake of brevity, the AP notes the following with respect to Fine Policy AP 2019. If the AP would have had to impose a fine using this policy, given Uber's global turnover and thus the large size of it as an offender, the AP would have seen cause to apply Article 8.4 of the Fine Policy Rules AP 2019. Indeed, setting penalty amounts within the penalty band of the AP 2019 Penalty Policies would in that case not result in an appropriate punishment that would be effective, proportionate and dissuasive. In conclusion, the AP would have imposed a fine of the same amount under force of the Fine Policy Rules 2019.



AUTORITEIT
PERSOONSGEGEVENS

Date
July 22,

Our
reference

6. Decision

Fine

The AP is imposing on Uber B.V. and Uber Technologies Inc. jointly, for violation of Art. 44. GDPR an administrative fine in the amount of €290,000,000 (in words: two hundred ninety million euros).¹²⁵

Sincerely,
Personal Data Authority,

w.g.

Mr. A. Wolfsen
Chairman

Remedies clause

If you disagree with this decision, you can submit a notice of objection digitally or on paper to the Personal Data Authority within six weeks from the date the decision was sent. Pursuant to Article 38 of the UGDPR, filing an objection suspends the effect of the decision imposing the administrative fine. To submit an objection digitally, see www.autoriteitpersoonsgegevens.nl, under the Contact heading, item "Objection or complaint about the AP."¹²⁶

The address for paper submission is:

Personal Data Authority
P.O. Box 93374
2509 AJ The Hague.

Mark the envelope "Awb objection" and put "objection" in the title of your letter. In

your objection letter, write at least:

- your name and address;
- the date of your objection;
- the reference (case number) mentioned in this letter, or attach a copy of this decision;
- The reason(s) why you disagree with this decision;
- your signature.

¹²⁵ The AP will hand the claim over to the Central Judicial Collection Agency (CJIB). The AP will not proceed with collection of the fine until any legal (follow-up) proceedings regarding this decision have been completed.



AUTORITEIT
PERSOONSgegevens

Date

July 22,

Our

reference

¹²⁶ The direct URL is <<https://www.autoriteitpersoonsgegevens.nl/over-de-autoriteit-persoonsgegevens/bezwaar-maken>>.